

CMP-WNROUT41



MANUAL (p. 2)
Wireless 11N router 300M

ANLEITUNG (S. 10)
11n WLAN Router 300 MBit

MODE D'EMPLOI (p. 19)
Routeur de réseau sans fil 11N 300M

GEBRUIKSAANWIJZING (p. 28)
Draadloze 11N router 300M

MANUALE (p. 36)
Router Wireless 11N 300M

MANUAL DE USO (p. 44)
Router inalámbrico 11N 300M

HASZNÁLATI ÚTMUTATÓ (o. 52.)
Vezeték nélküli 11N útválasztó 300M

KÄYTTÖOHJE (s. 60)
Langaton 11N reititin 300M

BRUKSANVISNING (s. 68)
Trådlös router 11N 300 m

NÁVOD K POUŽITÍ (s. 76)
Bezdrátový 11N router 300M

MANUAL DE UTILIZARE (p. 84)
Router wireless 11N 300M

ΕΓΧΕΙΡΙΔΙΟ ΧΡΗΣΗΣ (σελ. 92)
Ασύρματο router 11N 300M

BRUGERVEJLEDNING (s. 101)
Wireless 11N router 300M

VEILEDNING (s. 109)
Trådløs 11N router 300M

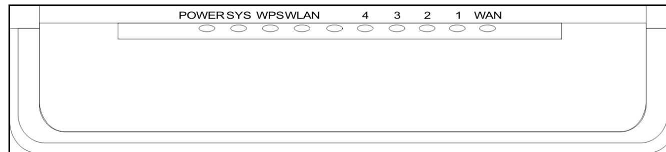
30-03-2012

ENGLISH

Chapter 1: Introduction

1.1 LED Indicator and Port Description

Front Panel and LED Indicator Display



LED indicator description on front panel: (from L to R)

- **POWER**

  When the green light stays on, it indicates that the power is connected properly.

- **SYS**

  When the green light is blinking, it indicates that the system is running properly.

- **WPS**

  When it is blinking, it indicates that the device is negotiating with the client in WPS mode.

- **WLAN**

  Wireless signal LED indicator. When the green light is blinking, it indicates that the wireless function is enabled.

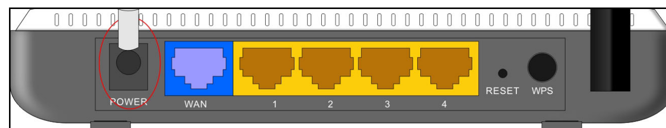
- **LAN (4, 3, 2, 1)**

  Wired local network LED indicator. If it stays on, it indicates that it is connected to the Ethernet device; blinking indicates that the device is transmitting and/or receiving data.

- **WAN**

  Wide area network indicator. If it stays on, it indicates the Router's W.

Back Panel Display:



Rear Panel: (From L to R)

- **POWER**

The jack is for power adapter connection. Please use the supplied 9V DC power adapter.

- **WAN**

A 100Mbps Ethernet port that can be connected with MODEM, Switch, Router and other Ethernet devices for Internet connection to DSL MODEM, Cable MODEM and ISP.

- **LAN (1, 2, 3, 4)**

4 10/100Mbps Ethernet ports can be connected with Ethernet switch, Ethernet router and NIC card.

- **RESET**

The system reset button. Press this button for 7 seconds, the settings configured in this device will be deleted and it will restore the default settings.

- **WPS**

Press it for 1 second, the WPS feature will be enabled and the WPS indicator will blink.

Chapter 2: Hardware Installation

2.1 How to Install the Router

Please use the supplied power adapter to power on the Router. IMPORTANT: Using a different power adapter could cause damage and void the warranty for this product. Please connect the LAN port of the Router to the network adapter of your computer with a cable. Please connect your broadband line provided by your ISP to the WAN port. Insert the supplied CD-ROM into the CD-ROM drive, double click the “Setup” icon and follow the instructions to complete the installation. Or you can enter the Router’s Web page to configure it. (For more details, please refer to Chapter 3.)

Chapter 3: How to Login to the Router

3.1 How to Set the Network Configurations

1. On your computer desktop, right-click “My Network Places” and select “Properties”.
2. Right-click “Local Area Network Connection” and select “Properties”.
3. Select “Internet Protocol (TCP/IP)” and click “Properties”.
4. - Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Click “OK” to save the configurations.
   - Or select “Use the following IP address” and enter the IP address, Subnet mask, and Default gateway as follows: IP Address: 192.168.0.XXX: (XXX is a number from 2~254) Subnet Mask: 255.255.255.0. Gateway: 192.168.0.1. You definitely need to input the DNS server address provided by your ISP. Otherwise, you can use the Router’s default gateway as the DNS proxy server. Click “OK” to save the configurations.

3.2 Login to the Router

1. To access the Router’s Web-based interface, launch a web browser such as Internet Explorer or Firefox and enter the Router’s default IP address, http://192.168.0.1. Press “Enter”.
2. Input the “admin” in both User Name and Password. Click “OK”.

default setting	
IP address	192.168.0.1
Password	admin
SSID	KONIG
Security Mode	Disable
Wireless Mode	b/g/n Mixd Mode
Channel	Autoselect
Time Zone	
WPS settings	Enable
UPNP Device Name	11N Wireless Broadband Router
UPNP Manufacturer	KONIGELECTRONIC
UPNP Model Name	CMP-WNROUT41
UPNP Model Number	V 1.0
UPNP reported network speed	300Mbps
UPNP Device address	http://192.168.0.1
UPNP	Disable

Chapter 4: Quick Setup Guide

4.1 Setup Wizard

Here is the "Welcome to Setup Wizard" for quick configuration of your Router. Click "Next".

In this screen, select one mode of Internet connection that you use. If you are not sure, press the "Detect" button or contact your Internet Service Provider, and click "Next".

ADSL Virtual Dial-up (Via PPPoE)

Enter the Account and Password provided by your ISP, and click "Next".

Dynamic IP (Via DHCP)

If your connection mode is Dynamic IP, it means your IP address keeps changing every time you connect. You do not need to enter the information like other modes. Click "Next" and "Save" to finish the settings.

Static IP

In this screen, enter the network address information from your ISP in the IP Address, Subnet Mask, Gateway and Primary DNS server fields and click "Next".

L2TP

Consult your ISP for the required information.

Chapter 5: Advanced Settings

5.1 LAN Settings

LAN Settings are for the basic TCP/IP parameters of LAN ports.

- **IP Address**: The Router's LAN IP addresses (not your PC's IP address). 192.168.0.1 is the default value.
- **Subnet Mask**: It shows the Router's subnet mask for measuring the network size. 255.255.255.0 is the default value.

IMPORTANT:

Once you modify the IP address, you need to remember it for the Web-based Utility login next time.

5.2 WAN Settings

After you have selected the ISP connection type in "Setup Wizard" and you want to modify the related settings, you can modify and configure the settings in detail here .

Static IP

If static IP is chosen as connection mode, you can modify the following address information.

- **IP Address**: Enter the WAN IP address provided by your ISP here.
- **Subnet Mask**: Enter the WAN Subnet Mask here.
- **Gateway**: Enter the WAN Gateway here.
- **Primary DNS Server**: Enter the Primary DNS server provided by your ISP.
- **Secondary DNS Server**: Enter the secondary DNS.

Chapter 6: Wireless Setting

6.1 Basic Settings

- **Enable Wireless**: Check to enable the Router's wireless features; uncheck to disable it.
- **Network Mode**: Select one mode from the following. The default is 11b/g/n mode.
- **Main SSID**: SSID (Service Set Identifier) is the unique name of the wireless network. This device has two SSIDs and the main SSID is necessary.
- **Minor SSID**: This is optional.
- **Broadcast (SSID)**: Select "Enable" to enable the device's SSID to be visible to wireless clients. The default is enabled.

- **MBSSID AP Isolation**: One access control feature based on wireless MAC address. When this feature is enabled, wireless clients connected to the same SSID cannot communicate with each other.
- **AP Isolation**: One access control feature based on SSID. When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. When this feature is enabled, wireless clients connected to the Main SSID and Minor SSID cannot communicate with each other, which can strongly secure the wireless network.
- **Channel**: Specify the effective channel (from 1 to 13\Auto) of the wireless network.
- **Extension Channel**: To increase data throughput of the wireless network, the extension channel range is used in 11n mode.
- **Channel Bandwidth**: Select the channel bandwidth to improve the wireless performance. When the network has 11b/g and 11n clients, you can select the 40M; when it is an 11n network, select 20/40M to improve its throughput.

6.2 Wireless Security Settings

This is used to configure the AP network's security setting. Here the six (ten in all) common encryption methods are presented, including Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2-enterprise, etc.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorised wireless devices from monitoring your transmissions or using your wireless resources. Select Mixed WEP to enter the following window:

- **Select SSID**: Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **Security Mode**: From the drop-down menu, select the corresponding security encryption modes.
- **WEP Key1~4**: Set the WEP key with the ASCII and Hex format. You can enter ASCII code (5 or 13 ASCII characters. Illegal characters such as "/" are not allowed.) or 10/26 hex characters.
- **Default Key**: Select one key from the four configured keys as the current available one.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. It applies more powerful encryption types (such as TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]) and can change the keys dynamically on every authorised wireless device.

- **Select SSID**: Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **WPA Algorithms**: Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Pass Phrase**: Enter the encrypted characters with 8-63 ASCII characters.
- **Key Renewal Interval**: Set the key's renewal period.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) provides higher security than WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access).

- **Select SSID**: Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **WPA Algorithms**: Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Pass Phrase**: Enter the encrypted characters with 8-63 ASCII characters.

- **Key renewal Interval**: Set the key's renewal period.

6.2.4 WPA- Enterprise

This security mode is used when a RADIUS server is connected to the device. Select "WPA-Enterprise" from the drop-down menu to enter the following window:

- **Select SSID**：Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **WPA Algorithms:** Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Key Renewal Interval**: Set the key's renewal period.
- **Radius Server**: Enter the IP address of the Radius server.
- **Radius Server port**: Enter the authentication port of the Radius server. The default is 1812.
- **Shared Secret**: Enter the shared key for the authentication server with 8~63 ASCII characters.
- **Session Timeout**: The authentication interval period between AP and authentication server.

6.2.5 WPA2-Enterprise

This security mode is based on Radius authentication server and WPA2 encryption method. WPA2 is used when a RADIUS server is connected to the device. Select "WPA2-Enterprise" from the drop-down menu to enter the following window:

- **Select SSID**: Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **WPA Algorithms**: Provides TKIP [Temporal Key Integrity Protocol] or AES [Advanced Encryption Standard]. The default is TKIP mode.
- **Key Renewal Interval**: Set the key's renewal period.
- **Radius Server**: Enter the IP address of the Radius server.
- **Radius Server port**: Enter the authentication port of the Radius server. The default is 1812.
- **Shared Secret**: Enter the shared key for the authentication server with 8~63 ASCII characters.
- **Session Timeout**: The authentication interval period between AP and authentication server. The default is 3600s.

6.2.6 802.1X

This security mode is used when a RADIUS server is connected to the device. 802.1x, a kind of port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physical port or logical port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port is not authenticated successfully, you can keep this port "disabled" which allows only 802.1x authentication protocol messages to pass. Select "802.1x" from the drop-down menu to enter the following window:

- **Select SSID**: Select the SSID (main SSID or minor SSID) to configure security settings from the drop-down menu.
- **WEP**: Click "Enable/Disable" to enable or disable the WEP algorithm.
- **Radius Server**: Enter the IP address of the Radius server.
- **Radius Server Port**: Enter the authentication port of the Radius server. The default is 1812.
- **Shared Secret**: Enter the shared key for the authentication server with 8~63 ASCII characters.
- **Session Timeout**: The authentication interval period between AP and authentication server. The default is 3600s.

6.4 WPS Settings

WPS (Wi-Fi Protected Setting) can be used to easily and quickly establish the connection between the wireless network clients and the device through encrypted contents. The users only enter a PIN code or press

the WPS button on the panel to configure it without manually selecting an encryption method and secret keys. In the “Wireless settings” menu, click “WPS settings” to enter the next screen.

- **WPS settings**: To enable or disable the WPS function. The default is “disable”.
- **WPS mode**: Provides two ways: PBC (Push-Button Configuration) and PIN code.
- **PBC**: Select the PBC or press the WPS button on the front panel of the device for about one second (Press the button for about one second and the WPS indicator will blink for 2 minutes, which means the WPS is enabled. While it is blinking, you can enable another device to implement the WPS/PBC negotiation between them. After two minutes, the WPS indicator will turn off, which means the WPS connection is completed. If more clients are added, repeat the above steps. At present, the WPS supports access of up to 32 clients.)
- PIN: If this option is enabled, you need to enter a wireless client’s PIN code in the field and keep the same code in the WPS client.

6.5 WDS Settings

The WDS (Wireless Distribution System) is used to expand the wireless coverage area. This Router provides three modes: Lazy, Bridge and Repeater.

Lazy: In this mode, the connected device can be in Bridge mode or Repeater mode, and enter the Router’s BSSID to establish the connection.

Bridge: You can wirelessly connect two or more wired networks via this mode. In this mode, you need to add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table.

Repeater Mode: In this mode, add the opposing MAC address into each own AP MAC address table manually or via scanner to enlarge and extend the wireless radio.

Chapter 7: DHCP Server

7.1 DHCP Settings

The DHCP (Dynamic Host Control Protocol) assigns an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer on the premise of activating “Obtain an IP Address Automatically”. So specifying the starting and ending address of the IP Address pool is needed.

- **DHCP Server**: Activate the checkbox to enable the DHCP server.
- **IP Address Start/End**: Enter the range of IP address for DHCP server distribution.
- **Lease Time**: The length of the IP address lease.

Chapter 8: Upgrade Firmware

8.1 The Router provides the firmware upgrade by clicking “Upgrade” after browsing the firmware upgrade packet which you can download from www.nedis.nl

- **Browse**: click this button to select the upgrade file.
- **Upgrade**: click this button to start the upgrading process. After the upgrade is completed, the Router will reboot automatically.

8.2 Reboot the Router

Rebooting the Router makes the configured settings take effect or sets the Router again if the settings failed.

8.3 Password Change

This section is for setting a new user name and password to better secure your router and network.

- **User Name**: Enter a new user name for the device.
- **Old Password**: Enter the old password.
- **New Password**: Enter a new password.
- **Re-enter to Confirm**: Re-enter to confirm the new password.

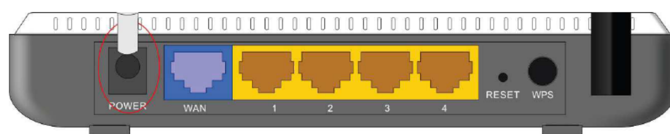
8.4 Logout

After you have finished the settings completely, click “Yes” on the logout page to logout from the web management page.

How to install and set-up a router on a cable or ADSL modem

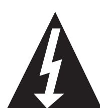
Caution!
Follow these steps without skipping a step

1. Switch the modem off (disconnect from mains power).
2. Switch the PC/laptop off.
3. Connect the **LAN output** of the modem via **LAN cable** to the **blue port** of the router.
4. Connect one of the **yellow ports** via **LAN cable** to the PC/laptop.



5. Now switch on the modem and wait until it is fully logged in (this can take a moment).
6. Switch on the router and wait at least 30 seconds.
7. Start up the PC/laptop and wait until it has completely booted.
8. Open your browser and navigate to http://192.168.0.1.
9. Enter user name and password (both by default: **admin**).
10. Navigate to the **Setup Wizzard** and click on **Auto Detect**.
11. Now click on **Next** and in the following screen click on **Apply**.
12. Navigate to the menu **WLAN settings** and ensure that **Enable Wireless** is checked.
13. Here you can configure your network name (SSID) and the channel.
14. Navigate to the submenu **Security Settings** and select the security type. We recommend to always select **Mixed WPA/WPA2 – Personal**.
15. Select **WPA Algorithms** as **TKIP&AES**.
16. Change the password in the field **Pass Phrase**. We recommend selecting a strong password consisting of letters, numbers and possibly 1 or more special characters.
17. Click on **Apply** to store the data.
18. Exit the browser screen; your wireless network and security settings are completed. Optionally you can disconnect the cable between router and PC/laptop to make a wireless connection (if the PC/laptop is equipped with a wireless receiver).

Safety precautions:






To reduce risk of electric shock, this product should ONLY be opened by an authorized technician when service is required. Disconnect the product from mains and other equipment if a problem should occur. Do not expose the product to water or moisture.

Maintenance:

Clean only with a dry cloth. Do not use cleaning solvents or abrasives.

Warranty:

No guarantee or liability can be accepted for any changes and modifications of the product or damage caused due to incorrect use of this product.

General:

- Designs and specifications are subject to change without notice.
- All logos brands and product names are trademarks or registered trademarks of their respective holders and are hereby recognized as such.
- This manual was produced with care. However, no rights can be derived. König Electronic can not accept liability for any errors in this manual or their consequences.
- Keep this manual and packaging for future reference.

Attention:



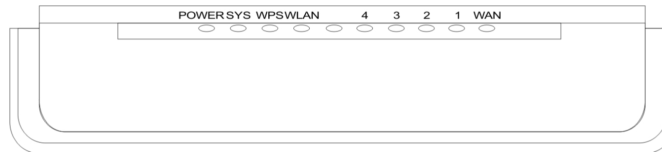
This product is marked with this symbol. It means that used electrical and electronic products should not be mixed with general household waste. There is a separate collections system for these products.

DEUTSCH

Kapitel 1: Einführung

1.1 LED-Anzeige und Beschreibung der Anschlüsse

Vorderseite und LED-Display



Beschreibung der LED-Anzeige auf der Vorderseite des Routers: (von links nach rechts)

- **POWER**

  Wenn das grüne Licht dauerhaft leuchtet, ist das Gerät ordnungsgemäß an die Stromversorgung angeschlossen.

- **SYS**

  Wenn das grüne Licht blinkt, funktioniert das System ordnungsgemäß.

- **WPS**

  Wenn diese Anzeige blinkt, kontaktiert das Gerät den Client im WPS-Modus.

- **WLAN**

  LED-Anzeige für drahtlose Signalübertragung. Wenn das grüne Licht blinkt, ist die drahtlose Signalübertragung aktiviert.

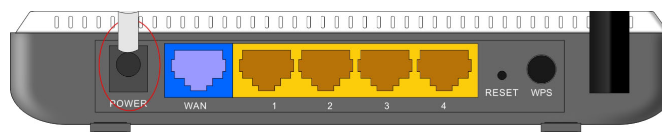
- **LAN (4, 3, 2, 1)**

  LED-Anzeige für drahtgebundenes lokales Netzwerk. Wenn die Anzeige dauerhaft leuchtet, besteht eine Verbindung zu dem Ethernet-Gerät. Wenn die Anzeige blinkt, sendet und/oder empfängt das Gerät Daten.

- **WAN**

  Anschluss zum Modem. Wenn die Anzeige dauerhaft leuchtet, befindet sich der Router im WAN-Modus.

Rückseite



Rückseite: (von links nach rechts)

- **POWER**

Dieser Anschluss ist der Netzanschluss. Bitte verwenden Sie das mitgelieferte Netzteil.

- **WAN**

Eine Ethernet-Schnittstelle mit einer Übertragungsrate von 100 Mbit/s, an die Sie ein Modem, Switch, Router und andere Ethernet-Geräte anschließen können, um eine Internetverbindung über ein DSL-Modem, Kabelmodem und ISP aufzubauen.

- **LAN (1, 3, 2, 4)**

Vier 10/100 MBit/s Ethernet-Schnittstellen, an die ein Ethernet-Switch, ein Ethernet-Router und Netzwerkkarten angeschlossen werden können.

- **RESET**

Reset-Taste. Drücken Sie diese Taste sieben Sekunden lang. Die vorgenommenen Einstellungen werden gelöscht und die Standardeinstellungen werden wiederhergestellt.

- **WPS**

Drücken Sie diese Taste eine Sekunde lang. WPS wird aktiviert und die WPS-Anzeige blinkt auf.

Kapitel 2: Installation der Hardware

2.1 Installation des Routers

Verwenden Sie nur das mitgelieferte Netzteil, um den Router mit Energie zu versorgen. WICHTIG: Die Verwendung eines anderen Netzteils kann den Router beschädigen und lässt die Garantieansprüche für dieses Produkt erlöschen. Verbinden Sie einen LAN-Anschluss des Routers mit einem Netzwerkkabel mit dem Netzwerkadapter Ihres Computers. Verbinden Sie ein DSL-Modem, das von Ihrem Provider zur Verfügung gestellt wurde, mit dem WAN-Port. Legen Sie die mitgelieferte CD-ROM in das CD-ROM-Laufwerk ein. Doppelklicken Sie auf das Symbol „Setup“ und folgen Sie den Anweisungen, um die Installation zu beenden. Alternativ können Sie den Router über dessen Webseite konfigurieren. (Weitere Informationen finden Sie in Kapitel 3.)

Kapitel 3: Log-in in den Router

3.1 Netzwerkeinstellungen vornehmen

1. Klicken Sie auf dem Desktop Ihres Computers mit der rechten Maustaste auf „Netzwerkumgebung“ und wählen Sie „Eigenschaften“.
2. Klicken Sie mit der rechten Maustaste auf „LAN-Verbindungen“ und wählen Sie „Eigenschaften“.
3. Wählen Sie „Internet-Protokoll (TCP/IP) “ und klicken Sie auf „Eigenschaften“.
4. - Wählen Sie „IP-Adresse automatisch beziehen“ und „DNS-Server-Adresse automatisch beziehen“. Klicken Sie auf „OK“, um die Einstellungen zu speichern.
   - Alternativ wählen Sie „Folgende IP-Adresse verwenden“ und geben Sie folgende IP-Adresse, Subnetzmaske und Standard-Gateway ein: IP-Adresse: 192.168.0.XXX: (XXX ist eine Zahl von 2-254) Subnetzmaske: 255.255.255.0.
   Gateway: 192.168.0.1. Sie müssen die DNS-Serveradresse, die von Ihrem Internetdienstanbieter zur Verfügung gestellt wurde, eingeben. Falls Sie diese nicht angeben, können Sie den Standard-Gateway Ihres Routers als Proxy-Server nutzen. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

3.2 Log-in in den Router

1. Um auf die Web-basierte Benutzeroberfläche des Routers zuzugreifen, starten Sie einen Webbrowser, wie Internet Explorer oder Firefox und geben Sie die Standard-IP-Adresse des Routers ein: http://192.168.0.1. Drücken Sie „Enter“.
2. Geben Sie sowohl bei Benutzername als auch bei Passwort „admin“ ein. Klicken Sie auf „OK“.

Standardeinstellungen	
IP-Adresse:	192.168.0.1
Passwort	admin
SSID	KONIG
Sicherheitsmodus	deaktiviert
Drahtlos-Modus	b/g/n Mixed Mode
Kanal	Autoselect
Zeitzone	
WPS-Einstellungen	aktiviert
UPNP Gerätename	11N Wireless Broadband Router
UPNP Hersteller	KONIGELECTRONIC
UPNP Modellname	CMP-WNROUT41
UPNP Modellnummer	V 1.0
UPNP gemeldete Netzwerkgeschwindigkeit	300 MBit/s

UPNP Geräteadresse	http://192.168.0.1
UPNP	deaktiviert

Kapitel 4: Kurzanleitung

4.1 Installationsassistent

Für die schnelle Installation Ihres Routers dient der Installationsassistent. Klicken Sie auf „weiter".

Wählen Sie in diesem Feld die Internetverbindung, die Sie benutzen. Wenn Sie sich nicht sicher sind, drücken Sie „suchen" oder kontaktieren Sie Ihren Internetdienstanbieter. Klicken Sie anschließend auf „weiter".

Virtueller ADSL-Verbindungsaufbau (über PPPoE)

Geben Sie den von Ihrem Internetdienstanbieter zur Verfügung gestellten Account und Passwort ein und klicken Sie anschließend auf „weiter".

Dynamische IP-Adresse (über DHCP)

Falls Ihr Verbindungsmodus dynamische IP-Adressen beinhaltet, wechseln Sie Ihre IP-Adresse immer dann, wenn Sie eine Internetverbindung herstellen. Sie müssen nicht, wie bei den anderen Verbindungsarten, Informationen eingeben. Klicken Sie auf „weiter" und „speichern", um die Einstellungen zu beenden.

Statische IP-Adresse

Geben Sie in diesem Feld die Informationen zur Netzwerkadresse Ihres Internetdienstanbieters, wie IP-Adresse, Subnetzmaske, Gateway und primärer DNS-Server ein und klicken Sie anschließend auf „weiter".

L2TP

Kontaktieren Sie Ihren Internetdienstanbieter, um die erforderlichen Informationen zu erhalten.

Kapitel 5: Erweiterte Einstellungen

5.1 LAN-Einstellungen

Die LAN-Einstellungen werden für die TCP/IP-spezifischen Grundparameter der LAN-Ports vorgenommen.

- **IP-Adresse**: Die LAN-IP-Adresse des Routers lautet wie folgt (nicht die PC-IP-Adresse): 192.168.0.1 ist die Voreinstellung.
- **Subnetzmaske**: Zeigt die Subnetzmaske des Routers, um die Netzwerkgröße zu messen. 255.255.255.0 ist die Voreinstellung.

WICHTIG:

Wenn Sie Ihre IP-Adresse ändern, müssen Sie sich diese merken, wenn Sie sich das nächste Mal in die Web-basiert Benutzeroberfläche einloggen möchten.

5.2 WAN-Einstellungen

Sobald Sie die nach dem jeweiligen Internetdienstanbieter spezifische Internetverbindung mit Hilfe des Installationsassistenten gewählt haben und Sie die damit verbundenen Einstellungen ändern wollen, können Sie dies unter diesem Menüpunkt tun.

Statische IP-Adresse

Wenn als Verbindungsmodus die statische IP-Adresse gewählt wurde, können Sie folgende Adressinformationen ändern.

- **IP-Adresse**: Geben Sie hier die WAN-IP-Adresse ein, die Ihnen von Ihrem Internetdienstanbieter zur Verfügung gestellt wurde.
- **Subnetzmaske**: Geben Sie hier die WAN-Subnetzmaske ein.
- **Gateway**: Geben Sie hier das WAN-Gateway ein.

- **Primärer DNS-Server**: Geben Sie den primären DNS-Server ein, der Ihnen von Ihrem Internetdienstanbieter zur Verfügung gestellt wurde.
- **Sekundärer DNS-Server**: Geben Sie den sekundären DNS-Server ein.

Kapitel 6: Drahtlose Netzwerkeinstellungen

6.1 Grundeinstellungen

- **Wireless aktivieren**: Markieren, wenn Sie die Wireless-Funktion des Routers aktivieren möchten. Entfernen Sie die Markierung, wenn Sie es deaktivieren möchten.
- **Netzwerkmodus**: Wählen Sie aus den folgenden Optionen: Die Grundeinstellung ist der 11b/g/n-Modus.
- **Main SSID**: SSID (Service Set Identifier) ist der Name eines Drahtlosnetzwerkes. Dieses Gerät verfügt über zwei SSID. Das „Main SSID“ ist obligatorisch.
- **Minor SSID**: Dieses SSID kann optional genutzt werden.
- **Broadcast (SSID)**: Wählen Sie „aktivieren“, um das SSID des Gerätes zu aktivieren und für den Wireless-Client sichtbar zu machen. In der Standardeinstellung ist das SSID aktiviert.
- **MBSSID AP Isolation**: Eine Zugriffskontrolle, die auf eine drahtlosen MAC-Adresse beruht. Wenn diese Funktion aktiviert ist, können die Wireless-Clients, die mit dem gleichen SSID verbunden sind nicht miteinander kommunizieren.
- **AP Isolation**: Eine Zugriffskontrolle, die auf SSID beruht. Wenn diese Funktion aktiviert ist, verfügt jeder Wireless-Client über ein eigenes virtuelles Netzwerk. Die Wireless-Clients können nicht miteinander kommunizieren. Wenn diese Funktion aktiviert ist, können die Wireless-Clients, die über den Main SSID und Minor SSID verbunden sind nicht miteinander kommunizieren. Dies erhöht die Sicherheit des Drahtlosnetzwerkes erheblich.
- **Kanal**: Bezeichnen Sie den aktiven Kanal (von 1 bis 13/Auto) des Drahtlosnetzwerkes.
- **Erweiterungskanal**: Um die Datenmenge im Drahtlosnetzwerk zu erhöhen, wird im 11n-Modus der erweiterte Satz von Kanälen verwendet.
- **Bandbreite des Kanals**: Wählen Sie die Bandbreite des Kanals, um die Leistungsfähigkeit der drahtlosen Übertragung zu verbessern. Wenn das Netzwerk über 11b/g- und 11n-Clients verfügt, wählen Sie 40M. Wenn es sich um ein 11n-Netzwerk handelt, wählen Sie 20/40M, um die Datendurchsatz zu erhöhen.

6.2 Wireless-Sicherheitseinstellungen

Diese Funktion wird verwendet, um die Sicherheitseinstellungen des Netzwerkes vorzunehmen. Im Folgenden werden dich sechs (zehn insgesamt) geläufigsten Verschlüsselungsmethoden vorgestellt. Dies beinhaltet gemischtes WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, etc.

6.2.1 Gemischtes WEP

WEP (Wired Equivalent Privacy) ist eine elementare Verschlüsselungsmethode, die Informationen, die drahtlos gesendet werden mit Hilfe einer Anzahl von digitalen Schlüsseln (mit einer Länge von 64 Bit oder 128 bis) verschlüsselt. Indem Sie bei jedem Ihrer drahtlosen Netzwerkgeräte die gleichen Schlüssel verwenden, werden nicht autorisierte Drahtlosgeräte davon abgehalten, dass Netzwerk zu nutzen oder Daten zu empfangen. Wählen Sie Mixed WEP, um zu dem folgenden Fenster zu gelangen:

- **SSID wählen**: Wählen Sie SSID (Main SSID oder Minor SSID), um die Sicherheitseinstellungen vom Drop-down-Menü vorzunehmen.
- **Sicherheitsmodus**: Wählen Sie aus dem Drop-down-Menü die entsprechende Sicherheitsverschlüsselung.
- **WEP Key 1~4**: Der WEP-Schlüssel wird im ASCII und Hex-Format angegeben. Sie können den Schlüssel als ASCII-Code (5 oder 13 ASCII-Zeichen, unzulässige Zeichen wie „/“ sind nicht erlaubt.) oder mit 10/26 Hex-Zeichen eingeben.
- **Standardschlüssel**: Wählen Sie aus den vier voreingerichteten Schlüsseln einen Schlüssel aus.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access) ist als Wi-Fi-Standard ein neueres Verschlüsselungsschema, welches die Sicherheitsmerkmale von WEP noch verbessern soll. WPA bedient sich leistungskräftigeren Verschlüsselungstechniken (wie TKIP [Temporal Key Integrity Protocol] oder AES [Advanced Encryption Standard]) und ändert die Schlüssel dynamisch auf jedem autorisierten Drahtlosgerät.

- **SSID wählen**: Wählen Sie SSID (Main SSID oder Minor SSID), um die Sicherheitseinstellungen vom Drop-down-Menü vorzunehmen.
- **WPA Algorithmus**: Unterstützt TKIP [Temporal Key Integrity Protocol] oder AES [Advanced Encryption Standard]. Als Standardeinstellung ist der TKIP-Modus aktiviert.
- **Passphrase**: Die verschlüsselten Zeichen werden als 8-63 ASCII-Zeichen eingegeben.
- **Zeitspanne für die Erneuerung der Schlüssel**: Legen Sie die Zeitspanne fest, nach der die Schlüssel erneuert werden.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access Version 2) bietet höhere Sicherheit als WEP (Wireless Equivalent Privacy) und WPA (Wi-Fi Protected Access).

- **SSID wählen**: Wählen Sie SSID (Main SSID oder Minor SSID), um die Sicherheitseinstellungen vom Drop-down-Menü vorzunehmen.
- **WPA Algorithmus**: Unterstützt TKIP [Temporal Key Integrity Protocol] oder AES [Advanced Encryption Standard]. Als Standardeinstellung ist der TKIP-Modus aktiviert.
- **Passphrase**: Die verschlüsselten Zeichen werden als 8-63 ASCII-Zeichen eingegeben.
- **Zeitspanne für die Erneuerung der Schlüssel**: Legen Sie die Zeitspanne fest, nach der die Schlüssel erneuert werden.

6.2.4 WPA- Enterprise

Dieser Sicherheitsmodus wird verwendet, wenn das Gerät mit einem RADIUS-Server verbunden ist. Wählen Sie aus dem Drop-down-Menü „WPA-Enterprise", um zu dem folgenden Fenster zu gelangen:

- **Wählen Sie SSID**：Wählen Sie SSID (Main SSID oder Minor SSID), um die Sicherheitseinstellungen vom Drop-down-Menü vorzunehmen.
- **WPA Algorithmus:** Unterstützt TKIP [Temporal Key Integrity Protocol] oder AES [Advanced Encryption Standard]. Als Standardeinstellung ist der TKIP-Modus aktiviert.
- **Zeitspanne für die Erneuerung der Schlüssel**: Legen Sie die Zeitspanne fest, nach der die Schlüssel erneuert werden.
- **RADIUS-Server:** Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS-Server-Anschluss:** Geben Sie die Authentifizierung für diesen Port des RADIUS-Servers ein. In der Standardeinstellung ist 1812.
- **Gemeinsamer geheimer Schlüssel**: Geben Sie mit 8~63 ASCII-Zeichen einen gemeinsamen geheimen Schlüssel für den Authentifizierungsserver ein.
- **Session Timeout:** Das Authentifizierungsintervall zwischen Access Point und Authentifizierungsserver.

6.2.5 WPA2-Enterprise

Dieser Sicherheitsmodus basiert auf einem Radius-Authentifizierungsserver und der WPA2-Verschlüsselungstechnik. WPA2 wird verwendet, wenn das Gerät mit einem RADIUS-Server verbunden ist. Wählen Sie aus dem Drop-down-Menü „WPA2-Enterprise", um zu dem folgenden Fenster zu gelangen:

- **SSID wählen:** Wählen Sie SSID (Main SSID oder Minor SSID), um die Sicherheitseinstellungen vom Drop-down-Menü vorzunehmen.
- **WPA Algorithmus:** Unterstützt TKIP [Temporal Key Integrity Protocol] oder AES [Advanced Encryption Standard]. Als Standardeinstellung ist der TKIP-Modus aktiviert.

- **Zeitspanne für die Erneuerung der Schlüssel**: Legen Sie die Zeitspanne fest, nach der die Schlüssel erneuert werden.
- **RADIUS-Server:** Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS-Server-Anschluss:** Geben Sie die Authentifizierung für diesen Port des RADIUS-Servers ein. In der Standardeinstellung ist 1812.
- **Gemeinsamer geheimer Schlüssel:** Geben Sie mit 8~63 ASCII-Zeichen einen gemeinsamen geheimen Schlüssel für den Authentifizierungsserver ein.
- **Session Timeout:** Das Authentifizierungsintervall zwischen Access Point und Authentifizierungsserver. Die Standardeinstellung ist 3600s.

6.2.6 802.1X

Dieser Sicherheitsmodus wird verwendet, wenn das Gerät mit einem RADIUS-Server verbunden ist. 802.1x, ist ein port-basiertes Authentifizierungsprotokoll und dient als Authentifizierungsart und -strategie für die Nutzer. Der Port kann entweder eine physische Schnittstelle oder ein logisches Port (wie VLAN) sein. Für die WLAN-Benutzer ist ein Port lediglich ein Kanal. Letztendlich ist das Ziel der 802.11x-Authentifizierung, zu überprüfen, ob der Port genutzt werden kann. Wenn der Port erfolgreich authentifiziert wird, können Sie dieses öffnen, alle Nachrichten werden weitergeleitet. Wenn der Port nicht erfolgreich authentifiziert wird, bleibt es deaktiviert, nur Nachrichten des 802.1x-Authentifizierungsprotokolls werden weitergeleitet. Wählen Sie aus dem Drop-down-Menü „802.1x“, um zu dem folgenden Fenster zu gelangen:

- **SSID wählen:** Wählen Sie SSID (Main SSID oder Minor SSID), um die Sicherheitseinstellungen vom Drop-down-Menü vorzunehmen.
- **WEP:** Klicken Sie auf „aktivieren/deaktivieren“, um den WEP-Algorithmus zu aktivieren oder zu deaktivieren.
- **RADIUS-Server:** Geben Sie die IP-Adresse des RADIUS-Servers ein.
- **RADIUS-Server-Anschluss:** Geben Sie die Authentifizierung für diesen Port des RADIUS-Servers ein. In der Standardeinstellung ist 1812.
- **Gemeinsamer geheimer Schlüssel:** Geben Sie mit 8~63 ASCII-Zeichen einen gemeinsamen geheimen Schlüssel für den Authentifizierungsserver ein.
- **Session Timeout:** Das Authentifizierungsintervall zwischen Access Point und Authentifizierungsserver. Die Standardeinstellung ist 3600s.

6.4 WPS-Einstellungen

WPS (Wi-Fi Protected Setting) wird verwendet um schnell und einfach eine Verbindung zwischen dem Wireless-Client und dem Gerät mittels verschlüsselter Inhalte herzustellen. Die Benutzer geben einfach nur eine PIN ein oder drücken die WPS-Taste auf dem Bedienfeld, ohne manuell eine Verschlüsselungsmethode oder geheime Schlüssel zu wählen. Klicken Sie im Menü „Wireless Settings“ auf „WPS Settings“, um zum nächsten Fenster zu gelangen.

- **WPS-Einstellungen:** Um die WPS-Funktion zu aktivieren oder zu deaktivieren. Die Standardeinstellung ist „deaktiviert“.
- **WPS-Modus:** Es gibt zwei Arten: PBC (Push-Button Configuration) und PIN-Code.
- **PBC:** Wählen Sie PBC oder drücken Sie eine Sekunde lang die WPS-Taste auf der Vorderseite des Gerätes (Drücken Sie die Taste ca. eine Sekunde lang und die WPS-Anzeige blinkt zwei Minuten lang. Die bedeutet, dass WPS aktiviert wurde. Während die Anzeige blinkt, können Sie andere Geräte für die WPS/PBC-Verbindung aktivieren. Nach zwei Minuten erlischt die WPS-Anzeige. Das bedeutet, dass die WPS-Verbindung hergestellt wurde. Wenn Sie mehrere Clients hinzufügen möchten, wiederholen Sie die soeben genannten Schritte. Derzeit können bis zu 32 Clients über WPS verbunden werden.)
- **PIN:** Wenn diese Option aktiviert wurde, müssen Sie den PIN-Code des Wireless-Client in das Feld eingeben und den gleichen Code für den WPS-Client verwenden.

6.5 WDS-Einstellungen

Das WDS (Wireless Distribution System) wird verwendet, um den Wireless-Empfangsbereich zu vergrößern. Dieser Router bietet drei verschiedene Betriebsarten: Lazy, Bridge und Repeater.

Lazy: In diesem Modus kann sich das verbundene Gerät im Bridge- oder Repeater-Modus befinden. Die BSSID des Routers wird für den Verbindungsaufbau verwendet.

Bridge: In diesem Modus können Sie drahtlos zwei oder mehr Drahtlosnetzwerke verbinden. In dieser Betriebsart müssen Sie die drahtlose MAC-Adresse des verbundenen Gerätes in die MAC-Adressen-Tabelle des Routers eingeben bzw. die entsprechende MAC-Adresse aus der Tabelle auswählen.

Repeater-Modus: In dieser Betriebsart müssen Sie die MAC-Adresse des jeweilig anderen Gerätes in die MAC-Adress-Tabelle manuell oder über den Scanner eintragen, um die Funkverbindung zu vergrößern und zu erweitern.

Kapitel 7: DHCP-Server

7.1 DHCP-Einstellungen

Beim DHCP (Dynamic Host Control Protocol) wird den Computern eines LAN/privaten Netzwerkes eine IP-Adresse zugewiesen. Wenn Sie den DHCP-Server aktivieren, weist dieser automatisch dem anfragendem Computer eine nicht benutzen IP-Adresse aus dem IP-Adresspool zu, vorausgesetzt folgende Funktion wurde aktiviert „IP-Adresse automatisch beziehen“. Der IP-Adresspool muss dazu näher spezifiziert werden.

- **DHCP-Server:** Klicken Sie in das entsprechende Kontrollkästchen, um den DHCP-Server zu aktivieren.
- **IP-Adresse Start/End**: Geben Sie den IP-Adressen-Bereich für die Zuweisung durch den DHCP-Server ein.
- **Lease Time**: Dies ist die Länger der Benutzungsdauer der IP-Adresse.

Kapitel 8: Upgrade der Firmware

8.1 Sie können die Firmware des Routers aktualisieren, indem Sie das Upgrade auf der Webseite www.nedis.nl herunterladen und anschließend auf „Upgrade“ klicken.

- **Browse**: Klicken Sie auf diese Schaltfläche, um die Upgrade-Datei zu wählen.
- **Upgrade**: Klicken Sie auf diese Schaltfläche, um das Upgrade zu starten. Nachdem das Upgrade durchgeführt wurde, führt der Router automatisch einen Neustart durch.

8.2 Neustart des Routers

Ein Neustart des Routers führt dazu, dass die durchgeführten Einstellungen aktiv werden. Falls die Einstellungen fehlgeschlagen sind, werden mit einem Neustart die ursprünglichen Einstellungen zurückgesetzt.

8.3 Änderung des Passwortes

Dieser Abschnitt handelt von der Änderung des Benutzernamens und des Passwortes, um Ihren Router und Ihr Netzwerk besser zu schützen.

- **Benutzername**: Geben Sie einen neuen Benutzernamen ein.
- **Altes Passwort**: Geben Sie das alte Passwort ein.
- **Neues Passwort**: Geben Sie das neue Passwort ein.
- **Bestätigen Sie das neue Passwort**: Geben Sie das neue Passwort erneut ein, um dieses zu bestätigen.

8.4 Abmelden

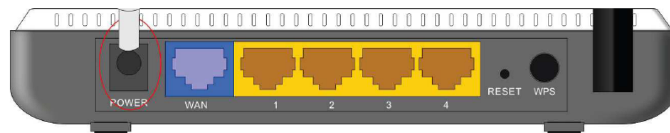
Nachdem Sie die Einstellungen erfolgreich vorgenommen haben, klicken Sie auf der Logout-Seite auf „Yes“, um sich abzumelden.

Anleitung zum Anschließen und Einrichten eines Routers an ein Kabel- oder ADSL-Modem

Vorsicht!

Befolgen Sie diese Schritte, ohne auch nur einen Schritt auszulassen

1. Schalten Sie das Modem aus (Ziehen Sie den Netzstecker).
2. Schalten Sie den PC/Laptop aus.
3. Verbinden Sie den **LAN-Ausgang** des Modems über ein **LAN-Kabel** mit dem **blauen Anschluss** des Routers.
4. Schließen Sie einen der **gelben Anschlüsse** über ein **LAN-Kabel** an den PC/Laptop an.



5. Schalten Sie nun das Modem ein und warten Sie, bis dieses vollständig eingeloggt ist (Dies kann eine Weile dauern.)
6. Schalten Sie den Router ein und warten Sie mindestens 30 Sekunden.
7. Schalten Sie den PC/Laptop ein und warten Sie bis dieser vollständig hochgefahren ist.
8. Öffnen Sie Ihren Browser und gehen Sie zu http://192.168.0.1.
9. Geben Sie den Benutzernamen und das Passwort ein (beides sind Standardeinstellungen: **admin**).
10. Öffnen Sie den **Installationsassistenten** und klicken Sie auf **Auto Detect**.
11. Klicken Sie jetzt auf **Weiter** und dann auf **Anwenden**.
12. Gehen Sie auf den Menüpunkt **WLAN-Einstellungen** und vergewissern Sie sich, dass **Drahtlosverbindung aktiviert** markiert ist.
13. An dieser Stelle können Sie Einstellungen zum Netzwerknamen (SSID) und dem Kanal vornehmen.
14. Öffnen Sie das Untermenü **Sicherheitseinstellungen** und wählen Sie den Sicherheitstyp. Wir empfehlen Ihnen **Mixed WPA/WPA2 – Personal** zu wählen.
15. Stellen Sie den **WPA-Verschlüsselungsalgorithmus** auf **TKIP&AES**.
16. Ändern Sie im Feld **Passwort** das Passwort. Wir empfehlen Ihnen, ein starkes Passwort zu wählen, welches aus Buchstaben, Ziffern und wenn möglich mindestens einem Sonderzeichen besteht.
17. Drücken Sie auf **Anwenden**, um die Einstellungen zu speichern.
18. Verlassen Sie Ihren Browser. Ihr Drahtlosnetzwerk und die Sicherheitseinstellungen wurden erfolgreich eingerichtet. Sie können das Kabel zwischen Router und PC/Laptop entfernen, um eine Drahtlosverbindung herzustellen (Dies gilt nur, wenn der PC/Laptop mit einem Funkempfänger ausgestattet ist.)

Sicherheitsvorkehrungen:



Um das Risiko eines elektrischen Schlags zu verringern, sollte dieses Produkt AUSSCHLIESSLICH von einem autorisierten Techniker geöffnet werden. Bei Problemen trennen Sie das Gerät bitte von der Spannungsversorgung und von anderen Geräten ab. Stellen Sie sicher, dass das Gerät nicht mit Wasser oder Feuchtigkeit in Berührung kommt.

Wartung:

Nur mit einem trockenen Tuch säubern. Keine Reinigungs- oder Scheuermittel verwenden.

Garantie:

Es kann keine Garantie oder Haftung für irgendwelche Änderungen oder Modifikationen des Produkts oder für Schäden übernommen werden, die aufgrund einer nicht ordnungsgemäßen Anwendung des Produkts entstanden sind.

Allgemeines:

- Design und technische Daten können ohne vorherige Ankündigung geändert werden.
- Alle Logos, Marken und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer und werden hiermit als solche anerkannt.
- Diese Bedienungsanleitung wurde sorgfältig verfasst. Dennoch können daraus keine Rechte und Pflichten hergeleitet werden. König Electronic haftet nicht für mögliche Fehler in dieser Bedienungsanleitung oder deren Folgen.
- Bitte bewahren Sie Bedienungsanleitung und Verpackung für spätere Verwendung auf.

Achtung:



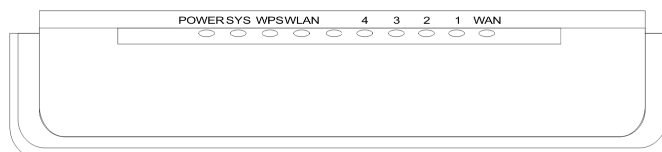
Dieses Produkt ist mit diesem Symbol gekennzeichnet. Es bedeutet, dass die ausgedienten elektrischen und elektronischen Produkte nicht mit dem allgemeinen Haushaltsmüll entsorgt werden dürfen. Für diese Produkte stehen gesonderte Sammelsysteme zur Verfügung.

FRANÇAIS

Chapitre 1 : Introduction

1.1 Indicateur lumineux et description des ports

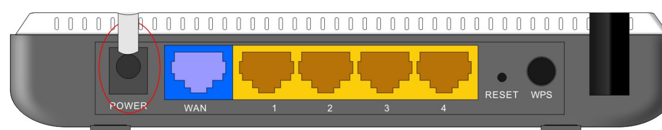
Panneau avant et affichage des indicateurs lumineux



Description des indicateurs lumineux du panneau avant : (de gauche à droite)

- **POWER (ALIMENTATION)**
  Lorsque le voyant lumineux vert reste allumé, il indique que l'appareil est correctement alimenté.
- **SYS (SYSTÈME)**
  Lorsque le voyant lumineux vert clignote, il indique que le système fonctionne correctement.
- **WPS (Configuration protégée WiFi)**
  Lorsqu'il clignote, il indique que l'appareil est en cours d'association avec le client en mode WPS.
- **WLAN (Réseau sans fil)**
  Indicateur lumineux de signal de réseau sans fil. Lorsque le voyant lumineux vert clignote, il indique que la fonction de réseau sans fil est active.
- **LAN (4, 3, 2, 1) (Réseau local)**
  Indicateur lumineux de réseau local câblé. S'il reste allumé, il indique que l'appareil est connecté au dispositif Ethernet ; lorsqu'il clignote, il indique que le dispositif transmet ou reçoit des données.
- **WAN (Réseau étendu)**
  Indicateur de réseau étendu. S'il reste allumé, il indique que le routeur est connecté au réseau étendu.

Vue du panneau arrière :



Panneau arrière : (de gauche à droite)

- **POWER (ALIMENTATION)**

Il s'agit de la prise de connexion de l'adaptateur d'alimentation. Veuillez utiliser l'adaptateur d'alimentation de 9 V DC fourni.

- **WAN (Réseau étendu)**

Il s'agit d'un port Ethernet à 100 MBit/s qui peut être connecté à un MODEM, à un commutateur, à un routeur ou à d'autres appareils Ethernet qui fournissent une connexion à Internet par un MODEM ADSL, par un MODEM câble ou par un fournisseur d'accès à Internet.

- **LAN (1, 2, 3, 4) (Réseau local)**

Il s'agit de 4 ports Ethernet 10/100 Mbit/s qui peuvent être connectés à un commutateur Ethernet, à un routeur Ethernet ou à une carte d'interface réseau.

- **RESET (RÉINITIALISATION)**

Il s'agit du bouton de réinitialisation du système. Appuyez sur ce bouton pendant 7 secondes, les paramètres définis dans ce dispositif seront effacés et les paramètres par défaut seront restaurés.

- **WPS (Configuration protégée WiFi)**

Appuyez sur ce bouton pendant 1 seconde, la fonction WPS sera activée et l'indicateur WPS se met à clignoter.

Chapitre 2 : Installation matérielle

2.1 Comment installer le routeur

Veuillez utiliser l'adaptateur d'alimentation fourni pour alimenter le routeur. IMPORTANT : L'utilisation d'un adaptateur d'alimentation différent peut endommager et annuler la garantie de ce produit. Veuillez connecter le port LAN (Réseau local) du routeur à la carte réseau de votre ordinateur à l'aide d'un câble. Veuillez connecter votre ligne Internet fournie par votre fournisseur d'accès Internet au port WAN (réseau étendu). Insérez le CD-ROM d'installation dans le lecteur de CD-ROM, double-cliquez l'icône « Setup » et suivez les instructions pour achever l'installation. Vous pouvez aussi accéder à la page Web du routeur pour le configurer. (Pour plus de détails, veuillez consulter le chapitre 3).

Chapitre 3 : Comment s'identifier auprès du routeur

3.1 Comment réaliser la configuration du réseau

1. Sur le bureau de votre ordinateur, cliquez avec le bouton droit de la souris sur « My Network Places » (Favoris réseau) et sélectionnez « Properties » (Propriétés).
2. Cliquez avec le bouton droit de la souris sur « Local Area Network Connection » (Connexion au réseau local) et sélectionnez « Properties » (Propriétés).
3. Sélectionnez « Internet Protocol (TCP/IP) » (Protocole Internet (TCP/IP)) et cliquez sur « Properties » (Propriétés).
4. - Sélectionnez « Obtain an IP address automatically » (Obtenir automatiquement une adresse IP) et « Obtain DNS server address automatically » (Obtenir automatiquement l'adresse d'un serveur DNS). Cliquez sur « OK » pour sauver la configuration.
   - Ou sélectionnez « Use the following IP address » (Utilisez l'adresse IP suivante) et saisissez l'adresse IP, le masque de sous-réseau et la passerelle par défaut comme il suit : Adresse IP : 192.168.0.XXX : (XXX est un nombre de 2 à 254) Masque de sous-réseau : 255.255.255.0.
   Passerelle : 192.168.0.1. Enfin, vous devez saisir l'adresse du serveur DNS fournie par votre fournisseur d'accès Internet. Autrement, vous pouvez utiliser la passerelle par défaut du routeur comme serveur proxy DNS. Cliquez sur « OK » pour sauver la configuration.

3.2 Identification auprès du routeur

1. Pour accéder à l'interface Web du routeur, lancez un navigateur web comme Internet Explorer ou Firefox et saisissez l'adresse IP par défaut de votre routeur c.à.d. http://192.168.0.1. Appuyez sur « Enter » (Entrer).
2. Saisissez « admin » comme nom d'utilisateur et comme mot de passe. Cliquez sur « OK ».

Configuration par défaut	
Adresse IP	192.168.0.1
Mot de passe	admin
SSID	KONIG
Mode de sécurité	Désactivé
Mode de réseau sans fil	Mode b/g/n Mixd
Canal	Sélection automatique
Fuseau horaire	
Configuration WPS	Activé
Nom du dispositif UPnP	11N Wireless Broadband Router (Routeur large bande sans fil 11N)
Fabricant UPnP	KONIGELECTRONIC
Nom du modèle UPnP	CMP-WNROUT41

Numéro de modèle UPnP	V 1.0
Débit du réseau reporté UPnP	300 MBit/s
Adresse du dispositif UPnP	http://192.168.0.1
UPnP	Désactivé

Chapitre 4 : Guide d'installation rapide

4.1 Setup Wizard - Assistant de configuration

Voici « Welcome to Setup Wizard » (Bienvenu dans l'assistant de configuration) pour la configuration rapide de votre routeur. Cliquez sur « Next » (Suivant).

Dans cet écran, sélectionnez le mode de connexion à Internet que vous utilisez. Si vous n'êtes pas certain, appuyez sur le bouton « Detect » (Détecter) ou contactez votre fournisseur d'accès Internet (FAI), et cliquez sur « Next » (Suivant).

ADSL Virtual Dial-up (Via PPPoE) - Connexion virtuelle ADSL (par PPPoE)

Saisissez le compte de l'utilisateur et le mot de passe obtenus auprès de votre FAI, et cliquez sur « Next » (Suivant).

Dynamic IP (Via DHCP) - IP Dynamique (par DHCP)

Lorsque votre mode de connexion est en dynamique IP, cela signifie que votre adresse IP est obtenue à chaque fois que vous vous connectez. Vous n'avez pas besoin de saisir des informations comme pour les autres modes. Cliquez sur « Next » (Suivant) et « Save » (Sauver) pour terminer la configuration.

Static IP - IP statique

Dans cet écran, saisissez les informations de l'adresse réseau fourni par votre FAI dans les champs Adresse IP, Masque de sous-réseau, Passerelle et Serveur Primaire DNS et cliquez sur « Next » (Suivant).

L2TP

Consultez votre FAI pour obtenir les informations nécessaires.

Chapitre 5 : Configurations avancées

5.1 Configuration LAN (Réseau local)

La configuration LAN concerne les paramètres de base TCP/IP des ports LAN (Réseau local).

- **IP address - Adresse IP** : Il s'agit de l'adresse IP sur le réseau local du routeur (non l'adresse IP de votre ordinateur PC). La valeur par défaut est 192.168.0.1.
- **Subnet Mask - Masque de sous-réseau** : Il indique le masque de sous-réseau du routeur pour dimensionner le réseau. La valeur par défaut est 255.255.255.0.

IMPORTANT :

Si vous modifiez l'adresse IP, vous devez la saisir à la prochaine identification avec l'utilitaire web.

5.2 Configuration WAN (Réseau étendu)

Après avoir sélectionné le type de connexion de votre FAI dans « Assistant de configuration »

Static IP - IP statique

Lorsqu'une adresse IP statique est choisi en tant que mode de connexion, vous pouvez modifiez la valeur de l'adresse suivante.

- **IP adress - Adresse IP** : Saisissez ici l'adresse IP WAN (Réseau étendu) fourni par votre FAI.
- **Subnet Mask - Masque de sous-réseau** : Saisissez ici le masque de sous-réseau WAN (Réseau étendu).
- **Gateway - Passerelle** : Saisissez ici l'adresse de la passerelle WAN (Réseau étendu).

- **Primary DNS Server - Serveur DNS Primaire** : Saisissez ici l'adresse IP du serveur DNS primaire fourni par votre FAI.
- **Secondary DNS Server - Serveur DNS Secondaire** : Saisissez l'adresse IP du serveur DNS secondaire.

Chapitre 6 : Configuration du réseau sans fil

6.1 Configuration de base

- **Enable Wireless - Activer le réseau sans fil** : Cochez la case pour activer la fonction de réseau sans file du routeur, décochez pour la désactiver.
- **Network Mode - Mode réseau** : Sélectionnez l'un des modes suivant. Le mode par défaut est le mode 11b/g/n.
- **Main SSID - SSID principal** : Le SSID (Service Set Identifier - Identifiant d'ensemble de service) est le nom unique du réseau sans fil. Ce dispositif possède deux SSID et seul le SSID principal est nécessaire.
- **Minor SSID - SSID secondaire** : C'est une valeur optionnelle.
- **Broadcast (SSID) - Diffusion (SSID)** : Sélectionnez « Enable » (Activé) pour rendre le SSID du dispositif visible aux clients de réseau sans fil. La diffusion est activée par défaut.
- **MBSSID AP Isolation - Isolement MBSSID AP** : C'est une fonction de contrôle d'accès basé sur l'adresse MAC du réseau sans fil. Quand cette fonction est activée, les clients du réseau sans fil connectés à un même SSID ne peuvent pas communiquer entre eux.
- **AP Isolation - Isolement AP** : C'est une fonction de contrôle d'accès basé sur l'identifant SSID. Quand cette fonction est activée, chacun de vos clients du réseau sans fil sera sur son propre réseau virtuel et ne sera pas en mesure de communiquer avec d'autres clients. Quand cette fonction est activée, les clients du réseau sans fil connectés au SSID principal ou au SSID secondaire ne peuvent pas communiquer entre eux, ce qui renforce la sécurité du réseau sans fil.
- **Channel - Canal** : Il définit le canal effectif (de 1 à 13 ou automatique) du réseau son fil.
- **Extension Channel - Canal de prolongement** : Pour augmenter le débit de données du réseau sans fil, la plage du canal de prolongement est utilisée en mode 11n.
- **Channel Bandwidth - Largeur de bande du canal** : Sélectionnez la largeur de bande du canal pour améliorer la performance du réseau sans fil. Quand le réseau contient des clients 11b/g et 11 n, vous pouvez sélectionner l'option 40M ; quand il s'agit d'un réseau avec des clients 11n, sélectionnez l'option 20/40M pour améliorer son débit.

6.2 Configuration de la sécurité du réseau sans fil

Ces paramètres permettent de configurer la sécurité du réseau à un point d'accès. Les six méthodes communes de chiffrement (dix au total) sont présentées ici, y comprise WEP mixte, WPA-personnel, WPA-entreprise, WPA2-personnel, WPA2-enterprise, etc.

6.2.1 Chiffrement WEP mixte

La méthode WEP (Wired Equivalent Privacy - Vie privé sur réseau sans fil équivalent), est une méthode de cryptage simple, habituellement elle crypte les données du réseau sans fil en utilisant une série de clés numériques (sur une longueur de 64 bits ou de 128 bits). En utilisant les mêmes clés sur chacun de vos dispositifs sur le réseau sans fil, vous pouvez empêcher les dispositifs du réseau sans fil non autorisés de surveiller vos transmissions ou d'utiliser vos ressources du réseau sans fil. Sélectionnez l'option « Mixed WEP » (WEP mixte) pour passer à la fenêtre suivante :

- **Select SSID - Sélection SSID** : Sélectionnez le SSID (SSID principal ou secondaire) pour définir la configuration de la sécurité dans le menu déroulant.
- **Security Mode - Mode de sécurité** : Dans le menu déroulant, sélectionnez la méthode de cryptage de la sécurité correspondante.

- **WEP Key1~4 - Clé WEP 1-4** : Définissez la clé WEP au format ASCII ou hexadécimal. Vous pouvez saisir une chaîne de caractère ASCII (de 5 ou 13 caractères. Les caractères illégaux comme le « / » ne sont pas autorisés) ou de 10/26 caractères hexadécimaux
- **Default Key - Clé par défaut** : Sélectionnez une clé parmi les quatre clés configurés comme l'une actuellement disponible.

6.2.2 WPA-Personal (WPA-Personnel)

La norme WPA (accès protégé WiFi), est une méthode de cryptage plus récente de réseau sans fil, conçu pour améliorer les fonctions de sécurité du chiffrement WEP. Elle implique des types de chiffrement plus robustes (comme TKIP [Temporal Key Integrity Protocol - Protocol d'intégrité de clé temporaire] ou AES [Advanced Encryption Standard -Norme de cryptage avancé]) et peut changer les clés dynamiquement de chaque dispositif autorisé du réseau sans fil.

- **Select SSID - Sélection SSID** : Sélectionnez le SSID (SSID principal ou secondaire) pour définir la configuration de la sécurité dans le menu déroulant.
- **WPA Algorithms - Algorithmes WPA** : Ils fournissent les algorithmes TKIP [Temporal Key Integrity Protocol - Protocol d'intégrité de clé temporaire] ou AES [Advanced Encryption Standard -Norme de cryptage avancé]. Le mode par défaut est TKIP.
- **Pass Phrase - Mot de passe** : Saisissez les caractères cachés sur 8-63 caractères ASCII.
- **Key Renewal Interval - Intervalle de renouvellement de clé** : Cela permet de définir la période de renouvellement de la clé.

6.2.3 WPA2- Personal (WPA2-Personnel)

La méthode WPA2 (Accès protégé WiFi version 2) offre une sécurité supérieure à la méthode WEP (Vie privée sur réseau sans fil équivalent) et WPA (Accès protégé WiFi).

- **Select SSID - Sélection SSID** : Sélectionnez le SSID (SSID principal ou secondaire) pour définir la configuration de la sécurité dans le menu déroulant.
- **WPA Algorithms - Algorithmes WPA** : Ils fournissent les algorithmes TKIP [Temporal Key Integrity Protocol - Protocol d'intégrité de clé temporaire] ou AES [Advanced Encryption Standard -Norme de cryptage avancé]. Le mode par défaut est TKIP.
- **Pass Phrase - Mot de passe** : Saisissez les caractères cachés sur 8-63 caractères ASCII.
- **Key Renewal Interval - Intervalle de renouvellement de clé** : Cela permet de définir la période de renouvellement de la clé.

6.2.4 WPA- Enterprise (WPA- Entreprise)

Ce mode de sécurité est utilisé lorsqu'un serveur RADIUS est connecté au dispositif. Sélectionnez « WPA-Enterprise » dans le menu déroulant pour saisir la fenêtre suivante :

- **Select SSID- Sélection SSID** : Sélectionnez le SSID (SSID principal ou secondaire) pour définir la configuration de la sécurité dans le menu déroulant.
- **WPA Algorithms - Algorithmes WPA** : Ils fournissent les algorithmes TKIP [Temporal Key Integrity Protocol - Protocol d'intégrité de clé temporaire] ou AES [Advanced Encryption Standard -Norme de cryptage avancé]. Le mode par défaut est TKIP.
- **Key Renewal Interval - Intervalle de renouvellement de clé** : Cela permet de définir la période de renouvellement de la clé.
- **Radius Server - Serveur RADIUS** : Saisissez l'adresse IP du serveur RADIUS.
- **Radius Server port- Port du serveur RADIUS** : Saisissez le port d'authentification du serveur RADIUS. La valeur par défaut est 1812.
- **Shared Secret - Clé secrète partagée** : Saisissez la clé partagée du serveur d'authentification sur 8 à 63 caractères ASCII.

- **Session Timeout - Durée de session** : Il s'agit de l'intervalle de durée d'authentification entre le point d'accès et le serveur d'authentification.

6.2.5 WPA2-Enterprise (WPA2-Entreprise)

Ce mode de sécurité est basé sur un serveur d'authentification Radius et une méthode de chiffrement WPA2. Le WPA2 est utilisé lorsqu'un serveur RADIUS est connecté sur le dispositif. Sélectionnez « WPA2-Enterprise » dans le menu déroulant pour saisir la fenêtre suivante :

- **Select SSID - Sélection SSID** : Sélectionnez le SSID (SSID principal ou secondaire) pour définir la configuration de la sécurité dans le menu déroulant.
- **WPA Algorithms - Algorithmes WPA** : Ils fournissent les algorithmes TKIP [Temporal Key Integrity Protocol - Protocol d'intégrité de clé temporaire] ou AES [Advanced Encryption Standard -Norme de cryptage avancé]. Le mode par défaut est TKIP.
- **Key Renewal Interval - Intervalle de renouvellement de clé** : Cela permet de définir la période de renouvellement de la clé.
- **Radius Server - Serveur RADIUS** : Saisissez l'adresse IP du serveur RADIUS.
- **Radius Server port- Port du serveur RADIUS** : Saisissez le port d'authentification du serveur RADIUS. La valeur par défaut est 1812.
- **Shared Secret - Clé secrète partagée** : Saisissez la clé partagée du serveur d'authentification sur 8 à 63 caractères ASCII.
- **Session Timeout - Durée de session** : Il s'agit de l'intervalle de durée d'authentification entre le point d'accès et le serveur d'authentification. La valeur par défaut est 3600 s.

6.2.6 Protocole 802.1X

Ce mode de sécurité est utilisé lorsqu'un serveur RADIUS est connecté au dispositif. Le protocole 802.1x est un type de protocole d'authentification à base de port. C'est un type d'authentification et une stratégie d'utilisateurs. Le port peut être soit un port physique, soit un port logique (comme VLAN). Pour les utilisateurs du réseau sans fil LAN (réseau local), un port est simplement un canal. Le but final de l'authentification 802.1x est de vérifier si le port peut être utilisé. Si le port est authentifié avec succès, vous pouvez ouvrir ce port ce qui permet tous les messages de passer. Si le port n'est pas authentifié avec succès, vous pouvez garder ce port « désactivé » ce qui permet aux messages sous le protocole d'authentification 802.1x de passer. Sélectionnez « 802.1x » dans le menu déroulant pour saisir la fenêtre suivante :

- **Select SSID - Sélection SSID** : Sélectionnez le SSID (SSID principal ou secondaire) pour définir la configuration de la sécurité dans le menu déroulant.
- **WEP** : Cliquez sur « Enable/Disable » (Activer/Désactiver) pour activer ou désactiver l'algorithme WEP.
- **Radius Server - Serveur RADIUS** : Saisissez l'adresse IP du serveur RADIUS.
- **Radius Server Port- Port du serveur RADIUS** : Saisissez le port d'authentification du serveur RADIUS. La valeur par défaut est 1812.
- **Shared Secret - Clé secrète partagée** : Saisissez la clé partagée du serveur d'authentification sur 8 à 63 caractères ASCII.
- **Session Timeout - Durée de session** : Il s'agit de l'intervalle de durée d'authentification entre le point d'accès et le serveur d'authentification. La valeur par défaut est 3600 s.

6.4 Configuration WPS

Le WPS (WiFi Protected Setting - Configuration WiFi protégée) peut être facilement et rapidement établit entre les clients du réseau sans fil et le dispositif par le biais de contenus cryptés. Les utilisateurs saisissent uniquement un code PIN ou appuient le bouton WPS sur le panneau pour le configurer sans sélectionner manuellement une méthode de cryptage et des clés secrètes. Dans le menu « Wireless settings » (Configuration du réseau sans fil), cliquez « WPS settings » (Configuration WPS) pour passer à l'écran suivant.

- **WPS settings - Configuration WPS** : Pour activer ou désactiver la fonction WPS. La valeur par défaut est « disable » (désactivé).
- **WPS mode - mode WPS** : Il fournit deux méthodes : PBC (Push-Bouton Configuration - Configuration par bouton-poussoir) et code PIN.
- **PBC** : Sélectionnez l'option PBC ou appuyez le bouton WPS sur le panneau avant du dispositif pendant environ une seconde (Appuyez le bouton pendant environ une seconde et l'indicateur WPS clignotera pendant 2 minutes, ce qui signifie que le mode WPS est activé). Alors qu'il est en train de clignoter, vous pouvez activer un autre dispositif pour implémenter une association WPS/PBC entre eux. Après deux minutes, l'indicateur WPS s'éteindra, ce qui signifie que la connexion WPS est complétée. Si plus de clients sont ajoutés, répétez les étapes ci-dessus. Actuellement, le mode WPS prend en charge un accès jusqu'à 32 clients.)
- PIN : Si l'option est activée, vous devez saisir le code PIN du client du réseau sans fil dans le champ et conserver le même code sur le client WPS.

6.5 Configuration WDS

Le WDS (Wireless Distribution System - Système de distribution sur réseau sans fil) est utilisé pour étendre la zone de couverture du réseau sans fil. Ce routeur propose trois modes : Lazy, Bridge (Pont) et Repeater (Répétiteur).

Lazy : Dans ce mode, le dispositif connecté peut être en mode Pont ou mode Répétiteur, et il faut saisir le BSSID du routeur pour établir une connexion.

Bridge - Pont : Vous pouvez connectez deux ou plusieurs réseaux câblés à l'aide de la transmission sans fil dans ce mode. Dans ce mode, vous devez ajouter l'adresse MAC du réseau sans fil du dispositif qui se connecte dans la table d'adresse MAC du point d'accès du routeur ou en sélectionnant un dans la table de détection.

Repeater Mode - Mode répétiteur : Dans ce mode, ajoutez manuellement ou par détection l'adresse MAC opposée dans chaque table d'adresse MAC propre, pour agrandir et étendre la couverture radio sans fil.

Chapitre 7 : Serveur DHCP

7.1 Configuration DHCP

Le protocole DHCP (Dynamic Host Control Protocol - Protocole de contrôle d'hôte dynamique) alloue une adresse IP à des ordinateurs sur le réseau LAN (local) ou privé. Quand vous activez le serveur DHCP, il allouera automatiquement une adresse IP non utilisée de la réserve d'adresse IP à l'ordinateur qui en fait la demande à condition d'activer l'option « Obtain an IP Address Automatically » (Obtenir une adresse IP automatiquement). Par conséquent, l'adresse de début et de fin de la réserve d'adresse IP sont nécessaires.

- **DHCP Server - Serveur DHCP** : Cochez la case pour activer le serveur DHCP.
- **IP Address Start/End - Adresse IP de début et de fin** : Entrez la plage d'adresse IP de distribution du serveur DHCP.
- **Lease Time - Temps alloué** : La durée d'allocation de l'adresse IP.

Chapitre 8 : Mise à niveau du micrologiciel

8.1 Le routeur peut être mis à niveau en cliquant sur « Upgrade » (Mise à niveau) après avoir sélectionné le paquet de mise à niveau du micrologiciel que vous pouvez télécharger sur www.nedis.nl

- **Browse - Explorer** : cliquez ce bouton pour sélectionner le fichier de mise à niveau.
- **Upgrade - Mise à nouveau** : cliquez ce bouton pour démarrer la procédure de mise à niveau. À la fin de la mise à niveau, le routeur redémarrera automatiquement.

8.2 Redémarrage du routeur

Grâce au redémarrage du routeur, la configuration définie est prise en compte ou vous pouvez reconfigurer le routeur si elle a échoué.

8.3 Changement du mot de passe

Ce paragraphe décrit la modification du nom de l'utilisateur et du mot de passe pour une meilleure sécurité de votre routeur et du réseau.

- **User Name - Nom d'utilisateur** : Saisissez un nouveau nom d'utilisateur pour le dispositif.
- **Old Password - Ancien mot de passe** : Saisissez l'ancien mot de passe.
- **New Password - Nouveau mot de passe** : Saisissez le nouveau mot de passe.
- **Re-enter to Confirm - Saisir à nouveau pour confirmer** : Saisissez à nouveau le nouveau mot de passe.

8.4 Fin de session

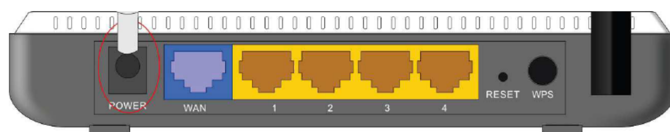
Après avoir fini entièrement la configuration, cliquez sur « Yes » (Oui) sur la page de fin de session pour fermer votre session sur la page web de gestion.

Comment installer et configurer un routeur pour câble ou de modem ADSL

Avertissement!

Suivez ces étapes sans en ignorer une

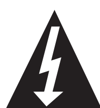
1. Éteignez le modem (débranchez-le de la source d'alimentation électrique).
2. Éteignez l'ordinateur personnel ou portable.
3. Branchez la **sortie LAN** du modem à l'aide **d'un câble réseau (LAN)** au **port bleu** du routeur.
4. Branchez l'un des **ports jaunes** à l'aide d'un **câble réseau (LAN)** à l'ordinateur personnel ou portable.



5. À présent, allumez le modem et patientez jusqu'à ce qu'il soit complétement connecté (la connexion peut prendre un certain temps).
6. Allumez le routeur et patientez au moins 30 secondes.
7. Allumez l'ordinateur personnel ou portable et patientez jusqu'à qu'il soit complétement démarré.
8. Ouvrez votre navigateur web et saisissez l'adresse http://192.168.0.1.
9. Saisissez le nom d'utilisateur et le mot de passe (les deux valeurs sont par défaut définies à: **admin**).
10. Allez sur **Setup Wizard** (Assistant de configuration) et cliquez sur **Auto Detect** (Détection automatique).
11. À présent, cliquez sur **Next** (Suivant) et cliquez sur **Apply** (Appliquer) de l'écran suivant.
12. Allez au menu **WLAN settings** (Configuration WLAN) et vérifiez que la case **Enable Wireless** (Activer le réseau sans fil) est cochée.
13. Dans ces champs, vous pouvez configurer votre nom de réseau (SSID) et le canal.
14. Allez au sous-menu **Security Settings** (Configuration de la sécurité) et sélectionnez le type de sécurité. Nous vous recommandons de sélectionner de préférence **Mixed WPA/WPA2 - Personal** (Mode mixte WPA/WPA2 - Personnel).
15. Sélectionnez **WPA Algorithms** (Algorithmes WPA) ainsi que **TKIP&AES**.
16. Changez le mot de passe dans le champ **Pass Phrase** (Mot de passe). Nous vous recommandons de saisir un mot de passe compliqué contenant des lettres, des nombres et si possible, 1 ou plusieurs caractères.
17. Cliquez sur **Apply** (Appliquer) pour sauvegarder les données.

18. Quittez le navigateur; votre réseau sans fil et la configuration de la sécurité sont complétés. Vous pouvez éventuellement débrancher le câble entre le routeur et l'ordinateur personnel ou portable pour établir la connexion sans fil (si l'ordinateur personnel ou portable est muni d'un récepteur).

Consignes de sécurité :






Pour réduire le risque de choc électrique, ce produit ne doit être ouvert que par un technicien qualifié si une réparation s’impose. Débranchez l’appareil et les autres équipements du secteur s’il y a un problème. Ne pas exposer l’appareil à l’eau ni à l’humidité.

Entretien :

Ne nettoyez l’appareil qu’avec un chiffon sec. N’utilisez pas de solvants ou de produits abrasifs.

Garantie :

Aucune garantie ou responsabilité ne sera acceptée en cas de modification et/ou de transformation du produit ou en cas de dommages provoqués par une utilisation incorrecte de l’appareil.

Généralités :

- Le design et les caractéristiques techniques sont sujets à modification sans notification préalable.
- Tous les logos de marques et noms de produits sont des marques déposées ou immatriculées dont leurs détenteurs sont les propriétaires et sont donc reconnues comme telles dans ce documents.
- Ce manuel a été produit avec soin. Toutefois, aucun droit ne peut en dériver. König Electronic ne peut être tenu responsable pour des erreurs de ce manuel ou de leurs conséquences.
- Conservez ce manuel et l’emballage pour toute référence ultérieure.

Attention :



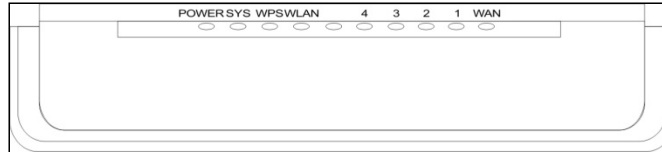
Ce symbole figure sur l’appareil. Il signifie que les produits électriques et électroniques ne doivent pas être jetés avec les déchets domestiques. Le système de collecte est différent pour ce genre de produits.

NEDERLANDS

Hoofdstuk 1: Inleiding

1.1 LED-indicator en poortbeschrijving

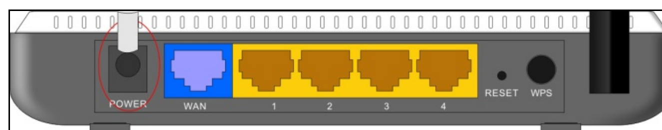
Voorpaneel en LED-indicator display:



Beschrijving van de LED-indicator op het voorpaneel: (van links naar rechts)

- **VOEDING**
  Wanneer de groene LED blijft branden, betekent dit dat de voeding correct is aangesloten.
- **SYS**
  Wanneer de groene LED knippert, betekent dit dat het systeem goed werkt.
- **WPS**
  Wanneer het knippert, betekent dit dat het apparaat onderhandelt met de client in de WPS-modus.
- **WLAN**
  Draadloos signaal LED-indicator. Wanneer de groene LED knippert, betekent dit dat de draadloze functie is ingeschakeld.
- **LAN (4, 3, 2, 1)**
  Bekabeld lokaal netwerk LED-indicator. Als het blijft branden, geeft het aan dat het met het Ethernet-apparaat is verbonden; knipperen geeft aan dat het apparaat gegevens aan het verzenden en/of ontvangen is.
- **WAN**
  Wide Area Netwerk indicator. Als het blijft branden, geeft het de W van de Router aan.

Achterpaneel display:



Achterpaneel: (van links naar rechts)

- **VOEDING**

De aansluiting is voor het aansluiten van de voedingsadapter. Gebruik de meegeleverde 9V DC-voedingsadapter.

- **WAN**

Een 100 Mbps Ethernetpoort die kan worden verbonden met de MODEM, Switch, Router en andere Ethernet-apparaten voor internetverbinding met DSL-MODEM, de KABELMODEM en ISP.

- **LAN (1, 2, 3, 4)**

De 4 10/100 Mbps Ethernet-poorten kunnen met Ethernet-switch, Ethernet-router en NIC-kaart worden verbonden.

- **RESETTEN**

De reset-knop van het systeem. Druk voor 7 seconden op deze knop, de instellingen die zijn geconfigureerd in dit apparaat zullen worden verwijderd en zal het de standaardinstellingen herstellen.

- **WPS**

Druk voor 1 seconde erop, de WPS-functie zal worden ingeschakeld en de WPS-indicator zal knipperen.

Hoofdstuk 2: Installatie van de hardware

2.1 De router installeren

Gebruik de bijgeleverde voedingsadapter om de router te voeden. BELANGRIJK: Het gebruik van een andere voedingsadapter kan schade veroorzaken en maakt de garantie voor dit product ongeldig. Sluit de LAN-poort van de Router met een kabel aan op de netwerkadapter van uw computer. Sluit uw breedbandaansluiting, door uw ISP geleverd, aan op de WAN-poort. Plaats de meegeleverde CD-ROM in het CD-romstation, dubbelklik op het “Setup”-pictogram en volg de instructies om de installatie te voltooien. Of u kunt de webpagina van de router invoeren om het te configureren. (Voor meer details, raadpleeg hoofdstuk 3.)

Hoofdstuk 3: Hoe op de router in te loggen

3.1 Hoe de netwerkconfiguraties in te stellen

1. Klik met de rechtermuisknop op “Mijn netwerklocaties” op het bureaublad van uw computer en selecteer “Eigenschappen”.
2. Klik met de rechtermuisknop op “LAN-verbinding” en selecteer “Eigenschappen”.
3. Selecteer “Internet Protocol (TCP/IP)” en klik op “Eigenschappen”.
4. - Selecteer “Automatisch een IP-adres verkrijgen” en “Automatisch een DNS-serveradres verkrijgen”. Klik op “OK” om de configuraties op te slaan.
   - Of selecteer “Gebruik het volgende IP-adres” en voer het IP-adres, subnetmasker en standaard gateway in als volgt: IP-adres: 192.168.0.XXX: (XXX is een getal van 2~254) Subnetmasker: 255.255.255.0.
   Gateway: 192.168.0.1. U moet beslist het adres van de DNS-server invoeren die uw ISP heeft verstrekt. Anders kunt u de standaard gateway van de router als de DNS-proxyserver gebruiken. Klik op “OK” om de configuraties op te slaan.

3.2 Inloggen op de router

1. Om de webgebaseerde interface van de router te benaderen, start een webbrowser zoals Internet Explorer of Firefox en voer het standaard IP-adres van de router in, http://192.168.0.1. Druk op “Enter”.
2. Voer “admin” in als gebruikersnaam en wachtwoord. Klik op “OK”.

Standaardinstelling	
IP-adres	192.168.0.1
Wachtwoord	admin
SSID	KONIG
Beveiligingsmodus	Uitschakelen
Draadloze modus	b/g/n gemengde modus
Kanaal	Automatische selectie
Tijdzone	
WPS-instellingen	Inschakelen
UPnP-apparaatnaam	11N draadloze breedband-router
UPnP-fabrikant	KONIGELECTRONIC
UPnP-modelnaam	CMP-WNROUT41
UPnP-modelnummer	V 1.0
UPNP gerapporteerde netwerksnelheid	300 Mbps
UPnP-apparaatadres	http://192.168.0.1
UPNP	Uitschakelen

Hoofdstuk 4: Beknopte installatiegids

4.1 Installatie-wizard

Hier is de “Welkom bij de installatie-wizard” voor een snelle configuratie van uw router. Klik op “Volgende”.

Selecteer in dit scherm één modus van internetverbinding die u gebruikt. Als u niet zeker bent, druk op de “Detect”-knop of neem contact op met uw Internet Service Provider en klik op “Volgende”.

ADSL virtuele Dial-up (via PPPoE)

Voer het account en wachtwoord in, verstrekt door uw ISP en klik op “Volgende”.

Dynamische IP (via DHCP)

Als uw verbindingsmodus dynamische IP is, betekent dit dat uw IP-adres blijft veranderen elke keer dat u verbinding maakt. U hoeft niet de gegevens zoals andere modi in te voeren. Klik op “Volgende” en “Opslaan” om de instellingen te voltooien.

Statische IP

Vul in dit scherm bij IP-adres, subnetmasker, Gateway en primaire DNS-server de netwerk-adresgegevens van uw ISP in en klik op “Volgende”.

L2TP

Raadpleeg uw ISP voor de vereiste informatie.

Hoofdstuk 5: Geavanceerde instellingen

5.1 LAN-instellingen

LAN-instellingen zijn voor de basis TCP/IP-parameters van LAN-poorten.

- **IP-adres:** De LAN IP-adressen van de router (niet uw IP-adres van uw PC). de standaardwaarde is 192.168.0.1.
- **Subnetmasker:** Het toont het subnetmasker van de router voor het meten van de grootte van het netwerk. de standaardwaarde is 255.255.255.0.

BELANGRIJK:

Zodra u het IP-adres wijzigt, moet u het voor de volgende keer voor het inloggen van de Web-based Utility onthouden.

5.2 WAN-instellingen

Nadat u de ISP-verbindingstype in de “Installatie-wizard” hebt geselecteerd en u wilt de bijbehorende instellingen wijzigen, kunt u de instellingen hier in detail wijzigen en configureren.

Statische IP

Als statische IP als verbindingsmodus is gekozen, kunt u de volgende adresgegevens wijzigen.

- **IP-adres:** Voer de WAN IP-adres verstrekt door uw ISP hier in.
- **Subnetmasker:** Voer hier het WAN-subnetmasker in.
- **Gateway:** Voer hier de WAN Gateway in.
- **Primaire DNS-server:** Voer de primaire DNS-server verstrekt door uw Internetprovider in.
- **Secundaire DNS-server:** Voer de secundaire DNS-server in.

Hoofdstuk 6: Draadloze instellingen

6.1 Basisinstellingen

- **Draadloos inschakelen:** Aanvinken om de draadloze functies van de router in te schakelen; afvinken om uit te schakelen.
- **Netwerkmodus:** Selecteer een modus uit het volgende. De standaardwaarde is 11b/g/n-modus.
- **Belangrijkste SSID:** De SSID (Service Set Identifier) is de unieke naam van het draadloze netwerk. Dit apparaat heeft twee SSID's en de belangrijkste SSID is vereist.

- **Secundaire SSID:** Deze is optioneel:
- **Uitzending (SSID):** Selecteer “Inschakelen” om de SSID van het apparaat voor draadloze client’s zichtbaar te maken. De standaard is ingeschakeld.
- **MBSSID AP isolatie:** Één toegangscontrolefunctie gebaseerd op draadloos MAC-adres. Wanneer deze functie is ingeschakeld, kunnen draadloze client’s aangesloten op dezelfde SSID niet met elkaar communiceren.
- **AP-isolatie:** Één toegangscontrolefunctie gebaseerd op SSID. Wanneer deze functie is ingeschakeld, zal elk van uw draadloze client’s in haar eigen virtuele netwerk zijn en zullen niet met elkaar kunnen communiceren. Wanneer deze functie is ingeschakeld, kunnen draadloze client’s aangesloten op de Belangrijkste SSID en Secundaire SSID niet met elkaar communiceren, wat het draadloze netwerk sterk kan beveiligen.
- **Kanaal:** Geef het effectieve kanaal (van 1 tot 13\Auto) van het draadloze netwerk op.
- **Extensiekanaal:** Om gegevensdoorvoer van het draadloze netwerk te verhogen, wordt het bereik van het extensiekanaal in de 11n-modus gebruikt.
- **Kanaalbandbreedte:** Selecteer de bandbreedte van het kanaal om de draadloze prestaties te verbeteren. Wanneer het netwerk 11b/g en 11n client’s heeft, kunt u de 40M selecteren; wanneer het een 11n netwerk is, selecteer 20/40M om de doorvoer te verbeteren.

6.2 Draadloze beveiligingsinstellingen

Dit wordt gebruikt voor het configureren van de beveiligingsinstelling van het AP-netwerk. Hier zijn de zes (tien in totaal) gebruikelijke coderingsmethoden gepresenteerd, waaronder gemengde WEP, WPA-personal, WPA-enterprise, WPA2-persoonlijk, WPA2-enterprise, enz.

6.2.1 Gemengde WEP

WEP (Wired Equivalent Privacy), een fundamentele coderingsmethode, codeert meestal draadloze gegevens met behulp van een reeks digitale sleutels (64 bits of 128 bits in lengte). Door dezelfde sleutels op elk van uw draadloze netwerkapparaten te gebruiken, kunt u voorkomen dat onbevoegde draadloze apparaten uw transmissies registreren of uw draadloze bronnen gebruiken. Selecteer gemengde WEP om het volgende venster te openen:

- **Selecteer SSID:** Selecteer de SSID (belangrijkste SSID of secundaire SSID) om beveiligingsinstellingen uit het pull-down menu te configureren.
- **Beveiligingsmodus:** Selecteer uit het pull-down menu de corresponderende beveiligingsmodi voor codering.
- **WEP=sleutel 1~4:** Stel de WEP-sleutel in met de ASCII- en Hex-formaat. U kunt ASCII-code (5 of 13 ASCII-tekens. Illegale karakters zoals “/” zijn niet toegestaan) of 10/26 hexadecimale tekens of 10/26 hexadecimale tekens invoeren.
- **Standaard sleutel:** Selecteer een sleutel van de vier geconfigureerde sleutels als de huidige beschikbare.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), een Wi-Fi-standaard, is een meer recente draadloze coderingregeling, ontworpen om de beveiligingsfuncties van WEP te verbeteren. Het past krachtigere coderingstypen toe (zoals TKIP [Temporal Key Integrity Protocol] of AES [Advanced Encryption Standard]) en kan op elke gemachtigde draadloos apparaat dynamisch de sleutels wijzigen.

- **Selecteer SSID:** Selecteer de SSID (belangrijkste SSID of secundaire SSID) om beveiligingsinstellingen uit het pull-down menu te configureren.
- **WPA algoritmen:** Biedt TKIP [Temporal Key Integrity Protocol] of AES [Advanced Encryption Standard]. De standaardwaarde is TKIP-modus.
- **Passphrase:** Voer de gecodeerde tekens met 8-63 ASCII-tekens in.

- **Sleutel vernieuwingsinterval:** Stel de vernieuwingsperiode van de sleutel in.

6.2.3 WPA2-Personal

WPA2 (Wi-Fi Protected Access versie 2) biedt hogere beveiliging dan WEP (Wireless Equivalent Privacy) en WPA (Wi-Fi Protected Access).

- **Selecteer SSID:** Selecteer de SSID (belangrijkste SSID of secundaire SSID) om beveiligingsinstellingen uit het pull-down menu te configureren.
- **WPA algoritmen:** Biedt TKIP [Temporal Key Integrity Protocol] of AES [Advanced Encryption Standard]. De standaardwaarde is TKIP-modus.
- **Passphrase:** Voer de gecodeerde tekens met 8-63 ASCII-tekens in.
- **Sleutel vernieuwingsinterval:** Stel de vernieuwingsperiode van de sleutel in.

6.2.4 WPA -Enterprise

Deze beveiligingsmodus wordt gebruikt als een RADIUS-server op het apparaat is aangesloten. Selecteer "WPA-Enterprise" in het pull-down menu om het volgende venster te openen:

- **Selecteer SSID**: Selecteer de SSID (belangrijkste SSID of secundaire SSID) om beveiligingsinstellingen uit het pull-down menu te configureren.
- **WPA algoritmen:** Biedt TKIP [Temporal Key Integrity Protocol] of AES [Advanced Encryption Standard]. De standaardwaarde is TKIP-modus.
- **Sleutel vernieuwingsinterval:** Stel de vernieuwingsperiode van de sleutel in.
- **RADIUS-server:** Voer het IP-adres van de RADIUS-server in.
- **RADIUS-serverpoort:** Voer de authenticatiepoort van de RADIUS-server in. De standaardwaarde is 1812.
- **Shared Secret**: Voer de gedeelde sleutel in voor de authenticatieserver met 8 ~ 63 ASCII-tekens.
- **Sessie Time-out**: De intervalperiode van authenticatie tussen AP en authenticatieserver.

6.2.5 WPA2-Enterprise

Deze beveiligingsmodus is gebaseerd op de RADIUS-authenticatieserver en WPA2 encryptiemethode. WPA2 wordt gebruikt als een RADIUS-server op het apparaat is aangesloten. Selecteer "WPA2-Enterprise" in het pull-down menu om het volgende venster te openen:

- **Selecteer SSID:** Selecteer de SSID (belangrijkste SSID of secundaire SSID) om beveiligingsinstellingen uit het pull-down menu te configureren.
- **WPA algoritmen:** Biedt TKIP [Temporal Key Integrity Protocol] of AES [Advanced Encryption Standard]. De standaardwaarde is TKIP-modus.
- **Sleutel vernieuwingsinterval:** Stel de vernieuwingsperiode van de sleutel in.
- **RADIUS-server:** Voer het IP-adres van de RADIUS-server in.
- **RADIUS-serverpoort:** Voer de authenticatiepoort van de RADIUS-server in. De standaardwaarde is 1812.
- **Shared Secret:** Voer de gedeelde sleutel in voor de authenticatieserver met 8 ~ 63 ASCII-tekens.
- **Sessie Time-out:** De intervalperiode van authenticatie tussen AP en authenticatieserver. De standaardwaarde is 3600 sec.

6.2.6 802.1X

Deze beveiligingsmodus wordt gebruikt als een RADIUS-server op het apparaat is aangesloten. 802. 1 x, een soort poortgebaseerde authenticatieprotocol, is een authenticatietype en strategie voor gebruikers. De poort kan ofwel een fysieke poort of en logische poort (zoals VLAN) zijn. Voor draadloze LAN-gebruikers, is een poort gewoon een kanaal. Het uiteindelijke doel van 802.11x-verificatie is om te controleren of de poort kan worden gebruikt. Als de poort met succes is geverifieerd, kunt u deze poort openen waarmee alle berichten kunnen worden doorgegeven. Als de poort niet met succes is geverifieerd, kun u deze poort "uitgeschakeld"

houden, waarmee alleen 802.1x authenticatieprotocol-berichten kunnen worden doorgegeven. Selecteer "802.1x" in het pull-down menu om het volgende venster te openen:

- **Selecteer SSID:** Selecteer de SSID (belangrijkste SSID of secundaire SSID) om beveiligingsinstellingen uit het pull-down menu te configureren.
- **WEP:** Klik op "Inschakelen/Uitschakelen"om het WEP-algoritme in of uit te schakelen.
- **RADIUS-server:** Voer het IP-adres van de RADIUS-server in.
- **RADIUS-serverpoort:** Voer de authenticatiepoort van de RADIUS-server in. De standaardwaarde is 1812.
- **Shared Secret:** Voer de gedeelde sleutel in voor de authenticatieserver met 8 ~ 63 ASCII-tekens.
- **Sessie Time-out:** De intervalperiode van authenticatie tussen AP en authenticatieserver. De standaardwaarde is 3600 sec.

6.3 WPS-instellingen

WPS (Wi-Fi Protected Setting) kan gebruikt worden om, via gecodeerde inhoud, gemakkelijk en snel de verbinding tussen de draadloze netwerkclient's en het apparaat tot stand te brengen. De gebruikers voeren alleen een pincode in of drukken op de WPS-knop op het paneel om het te configureren zonder handmatig een coderingsmethode en geheime sleutels te selecteren. Klik in het "Wireless-instellingen"-menu op "WPS-instellingen" om het volgende scherm te openen.

- **WPS-instellingen:** Om de WPS-functie in of uit te schakelen. De standaard is uitschakelen.
- **WPS-modus:** Biedt twee manieren: PBC (Push-Button Configuration) en PIN-code.
- **PBC:** Selecteer de PBC of druk voor ongeveer één seconde op de "WPS"-knop op het voorpaneel van het apparaat (Druk voor ongeveer één seconde op de knop en de WPS-indicator zal gedurende 2 minuten knipperen, wat betekent dat de WPS is ingeschakeld. Terwijl het knippert, kunt u een ander apparaat inschakelen om de WPS/PBC-onderhandelingen tussen hen uit te voeren. Na twee minuten, zal de WPS-indicator uitschakelen, wat betekent dat de WPS-verbinding is voltooid. Als meer client's worden toegevoegd, herhaal de bovenstaande stappen. Op dit moment ondersteunt de WPS toegang voor maximaal 32 client's.)
- PIN: Als deze optie is ingeschakeld, moet u een PIN-code van de draadloze client in het veld invoeren en dezelfde code in de WPS-client houden.

6.4 WDS-instellingen

De WDS (Wireless Distribution System) wordt gebruikt om het draadloze dekkingsgebied uit te breiden. Deze router biedt drie modi: Lazy, Bridge en Repeater.

Lazy: In deze modus kan het aangesloten apparaat in de Bridge- of Repeater-modus worden geschakeld en voer de BSSID van de router in om een verbinding tot stand te brengen.

Bridge: U kunt draadloos twee of meer bekabelde netwerken via deze modus verbinden. In deze modus moet u het draadloos MAC-adres van het aansluitende apparaat in het AP MAC-adrestabel van de router toevoegen of één uit de scantabel selecteren.

Repeater-modus: In deze modus, voeg handmatig het tegengestelde MAC-adres in elke eigen AP MAC-adrestabel toe of via de scanner om het draadloze radiobereik te vergroten en uitbreiden.

Hoofdstuk 7: DHCP-server

7.1 DHCP-instellingen

De DHCP (Dynamic Host Control Protocol) wijst een IP-adres aan de computers in het LAN/privénetwerk toe. Wanneer u de DHCP-Server inschakelt, zal de DHCP-server automatisch een ongebruikt IP-adres van de IP-adresgroep aan de aanvragende computer toewijzen onder voorwaarde van activering van "Automatisch een IP-adres verkrijgen". Dus is het specificeren van het start- en eindadres van de IP-adresgroep nodig.

- **DHCP-server:** Activeer het aankruisvak om de DHCP-server in te schakelen.
- **IP-adres start/eind:** Voer het bereik van het IP-adres voor DHCP-server distributie in.

■ **Leasetijd:** De lengte van de IP-adreslease.

Hoofdstuk 8: Upgraden van de firmware

8.1 De router biedt de firmware upgrade door op “Upgrade” te klikken die u na het surfen van het firmware-upgradepakket van www.nedis.nl kunt downloaden.

■ **Bladeren:** Klik op deze knop om het upgrade-bestand te selecteren.

■ **Upgrade:** Klik op deze knop om met het upgradeproces te beginnen. Nadat de upgrade is voltooid, zal de router automatisch herstarten.

8.2 Opnieuw opstarten van de router

Het opnieuw opstarten van de router zorgt ervoor dat de geconfigureerde instellingen van kracht worden of stelt de router opnieuw in als de instellingen mislukten.

8.3 Wachtwoord wijzigen

Deze sectie is voor het instellen van een nieuwe gebruikersnaam en wachtwoord om uw router en het netwerk beter te beveiligen.

■ **Gebruikersnaam:** Voer een nieuwe gebruikersnaam voor het apparaat in.

■ **Oud wachtwoord:** Voer het oude wachtwoord in:

■ **Nieuw wachtwoord:** Voer een nieuw wachtwoord in.

■ **Voer nogmaals in om te bevestigen:** Voer nogmaals in om het nieuwe wachtwoord te bevestigen

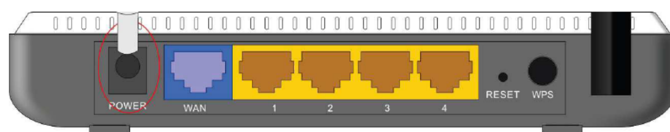
8.4 Uitloggen

Nadat u met de instellingen volledig klaar bent, klik op “Ja” op de uitlogpagina om uit de webbeheerpagina te loggen.

Het aansluiten en instellen van een router op een Kabel of ADSL Modem.

Let op!
Volg deze stappen stuk voor stuk en sla niets over

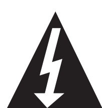
1. Schakel het Modem uit (Van de stroom af halen)
2. Schakel de PC/Laptop uit
3. Verbind nu de **LAN uitgang** van het Modem aan de **Blauwe poort** van de Router dmv een **LAN kabel**.
4. Verbind nu een van de **Gele poorten** met de PC/Laptop dmv een **LAN ka**bel.



5. Schakel nu het Modem in en wacht totdat deze geheel aangemeld is (dit kan enige tijd duren).
6. Schakel nu de router in en wacht minimaal 30 seconden
7. Start nu de PC/Laptop op en wacht tot deze geheel is opgestart
8. Open nu uw browser en ga naar http://192.168.0.1
9. Voer nu de gebruikersnaam en het wachtwoord in (Standaard zijn beide: **admin**)
10. Ga nu naar **Setup Wizzard** en klik op **Auto Detect**
11. Zodra deze klaar is klikt u op **Next** en in het volgende scherm op **Apply**
12. Ga nu naar het menu **WLAN settings** en zorg dat **Enable Wireless** aangevinkt is
13. Hier kunt u de naam van uw netwerk (SSID) en het zendkanaal aanpassen
14. Ga nu naar het submenu **Security Settings** en kies hier voor het soort beveiliging. Wij adviseren u altijd te kiezen voor **Mixed WPA/WPA2 – Personal.**
15. Kies bij **WPA Algorithms** voor **TKIP&AES**

16. Verander nu het wachtwoord in het veld van **Pass Phrase**. Wij adviseren u een sterk wachtwoord te kiezen bestaande uit letters cijfers en eventueel 1 of meerdere leestekens.
17. Klik nu op **Apply** en de gegevens worden opgeslagen.
18. Nu kunt u het browserscherm afsluiten en is uw netwerk draadloos en beveiligd ingesteld. U kunt desgewenst de kabel tussen de router en de PC/Laptop verwijderen en draadloos verbinding te maken (Indien de PC/Laptop is voorzien van een wireless ontvanger)

Veiligheidsvoorzorgsmaatregelen:






Om het risico op elektrische schokken te voorkomen mag dit product ALLEEN worden geopend door een erkende technicus wanneer er onderhoud nodig is. Koppel het product los van de elektrische voeding en van andere apparatuur als zich problemen voordoen. Stel het product niet bloot aan water of vocht.

Onderhoud:

Uitsluitend reinigen met een droge doek. Gebruik geen reinigingsmiddelen of schuurmiddelen.

Garantie:

Voor wijzigingen en veranderingen aan het product of schade veroorzaakt door een verkeerd gebruik van dit product, kan geen aansprakelijkheid worden geaccepteerd. Tevens vervalt daardoor de garantie.

Algemeen:

- Wijziging van ontwerp en specificaties zonder voorafgaande mededeling onder voorbehoud.
- Alle logo’s, merken en productnamen zijn handelsmerken of geregistreerde handelsmerken van de respectievelijke eigenaren en worden hierbij als zodanig erkend.
- Deze handleiding is met zorg samengesteld. Er kunnen echter geen rechten aan worden ontleend. König Electronic kan geen aansprakelijkheid aanvaarden voor eventuele fouten in deze handleiding of de gevolgen daarvan.
- Bewaar deze gebruiksaanwijzing voor latere raadpleging.

Let op:

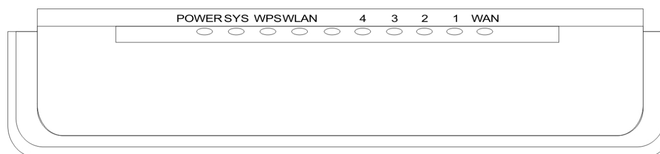


Dit product is voorzien van dit symbool. Dit symbool geeft aan dat afgedankte elektrische en elektronische producten niet met het gewone huisafval verwijderd mogen worden. Voor dit soort producten zijn er speciale inzamelingspunten.

Capitolo 1: Introduzione

1.1 Descrizione Indicatore LED e Porta

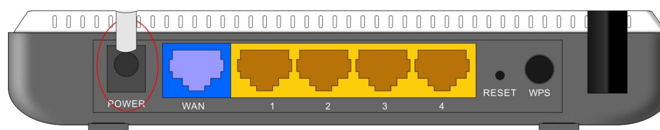
Pannello Frontale e Display indicatore LED



Descrizione indicatore LED sul pannello frontale: (da S a D)

- **ALIMENTAZIONE**
  Quando la luce verde è accesa, essa indica che l'alimentazione è connessa in modo adeguato.
- **SYS**
  Quando la luce verde è accesa, essa indica che il sistema sta funzionando in modo adeguato.
- **WPS**
  Quando lampeggia, essa indica che il dispositivo sta negoziando con il client in modalità WPS.
- **WLAN**
  Indicatore LED del segnale wireless. Quando la luce verde sta lampeggiando, essa indica che la funzione wireless è abilitata.
- **LAN (4, 3, 2, 1)**
  Indicatore LED della rete locale a cavo. Se rimane acceso, esso indica che è connesso con il dispositivo Ethernet; lampeggiando indica invece che il dispositivo sta trasmettendo e/o ricevendo dati.
- **WAN**
  Indicatore di ampia area di rete. Se rimane acceso indica la W del Router.

Visualizzatore Pannello Posteriore:



Pannello Posteriore: (da S a D)

- **ALIMENTAZIONE**

Il jack per la connessione dell'alimentatore. Vi preghiamo di usare l'alimentatore a 9V DC fornito.

- **WAN**

Una porta Ethernet a 100Mbps che può essere connessa con un MODEM, Selettore, Router ed altri dispositivi Ethernet per la connessione Internet ad un MODEM DSL, MODEM cavo e ISP.

- **LAN (1, 2, 3, 4)**

4 Porte Ethernet 10/100Mbps che possono essere connesse con un selettore Ethernet, un router Ethernet ed una scheda NIC.

- **RESET**

Il pulsante di reset del sistema. Premere questo pulsante per 7 secondi, i parametri configurati in questo dispositivo saranno cancellati ed esso si ripristinerà sulle impostazioni predefinite.

- **WPS**

Premere per 1 secondo, la caratteristica WPS sarà attivata e l'indicatore WPS lampeggerà.

Capitolo 2: Installazione hardware

2.1 Come installare il Router

Vi preghiamo di utilizzare l'alimentatore fornito sul Router. IMPORTANTE: Utilizzare un alimentatore differente potrebbe causare danni e quindi cancellare la garanzia per questo prodotto. Vi preghiamo di connettere la porta LAN del router all'adattatore di rete del vostro computer con un cavo. Vi preghiamo di connettere la vostro linea a banda larga fornitavi dal vostro ISP alla porta WAN. Inserire il CD-ROM fornito nel lettore di CD-ROM, fare doppio click sull'icona “Setup” e seguire le istruzioni per completare l'installazione. Oppure potete accedere alla pagina web del router per configurarlo. (per maggiori dettagli, vi preghiamo di far riferimento al capitolo 3)

Capitolo 3: Come accedere al Router

3.1 Come impostare le configurazioni di rete

1. Sul vostro desktop, cliccate con il tasto destro su “Mie posizioni di Rete” e quindi selezionate “proprietà”.
2. Cliccare con il tasto destro su “connessione di rete locale” e selezionare “Proprietà”.
3. Selezionare “Protocollo Internet (TCP/IP)” e cliccare su “Proprietà”.
4. - Selezionare “Ottieni l'indirizzo IP automaticamente” e “Ottiene l'indirizzo del server DNS automaticamente”. Cliccare su OK per salvare le configurazioni.
   - O selezionare “utilizza il seguente indirizzo IP” ed inserite l'indirizzo IP, la maschera Subnet ed il gateway predefinito come segue: Indirizzo IP: 192.168.0.XXX: (XXX è u numero compreso tra 2~254) Maschera Subnet: 255.255.255.0.
   Gateway: 192.168.0.1. Dovrete assolutamente inserire l'indirizzo del server DNS fornito dal vostro ISP. Altrimenti, potete utilizzare il gateway predefinito del router come server Proxy DNS. Cliccare su OK per salvare le configurazioni.

3.2 Accedere al Router

1. Per accedere all'interfaccia Web del router, eseguire un browser web come Internet Explorer o Firefox ed inserire il numero IP predefinito del Router, http://192.168.0.1. Premere “enter”.
2. Inserire “admin” sia per Nome Utente che Password. Quindi cliccare sul pulsante “OK”.

impostazioni predefinite	
Indirizzo IP	192.168.0.1
Password	admin
SSID	KONIG
Modalità di sicurezza	Disattivare
Modalità Wireless	b/g/n Modalità mista
Canale	Autoselezione
Fuso Orario	
Impostazioni WPS	Attivo
Numero dispositivo UPNP	Router a banda larga wireless 11N
UPNP Costruttore	KONIGELECTRONIC
UPNP Nome modello	CMP-WNROUT41
UPNP Numero Modello	V 1.0
UPNP velocità di rete riportata	300Mbps
UPNP Indirizzo Dispositivo	http://192.168.0.1
UPNP	Disattivare

Capitolo 4: Guida rapida di impostazione

4.1 Impostazione veloce

Qui si riporta il “Benvenuto all'impostazione veloce” per una configurazione rapida del vostro Router. Cliccare “Avanti”.

In questa schermata, selezionare una modalità di connessione internet da utilizzare. Se non siete sicuri, premete il pulsante “rileva” o contattate il vostro ISP, e cliccate su “Avanti”.

ADSL Dial-up virtuale (attraverso PPPoE)

Inserire il Conto e Password forniti dal vostro ISP e cliccate su “Avanti”.

IP Dinamico (Attraverso DHCP)

Se la vostra modalità di connessione è un IP dinamico, ciò significa che l'indirizzo IP cambierà ogni volta che vi connetterete. Non vi sarà bisogno di inserire le informazioni come accade per le altre modalità- Cliccare su “avanti” e “salva” per completare le impostazioni.

IP statico

In questa schermata, inserite l'informazione nei campi per l'indirizzo di rete dal vostro ISP nell'indirizzo IP, maschera subnet, Gateway e Server primario DNS e cliccate su “Avanti”.

L2TP

Consultare il vostro ISP per l'informazione richiesta.

Capitolo 5: Impostazioni Avanzate

5.1 Impostazioni LAN

Le impostazioni LAN sono per parametri base TCP/IP delle porte LAN.

- **Indirizzo IP**: Gli indirizzi IP LAN del router (non gli indirizzi IP del vostro PC). 192.168.0.1 è il valore predefinito.
- **Maschera Subnet**: Mostra la maschera subnet del router per la misurazione della dimensione di rete. 255.255.255.0 è il valore predefinito.

IMPORTANTE:

Una volta che si modifica l'indirizzo IP, necessitate di ricordarlo per l'accesso sull'utility basato su web la volta successiva.

5.2 Impostazioni WAN

Dopo che avete selezionato il tipo di connessione ISP nell' “Impostazione Veloce” e volete modificare le relative impostazioni, potete modificare e configurare le impostazioni in dettaglio.

IP statico

Se viene scelto l'IP statico come modalità di connessione, potete modificare la seguente informazione dell'indirizzo.

- **Indirizzo IP**: Inserire l'indirizzo IP WAN fornito da il vostro ISP qui.
- **Maschera Subnet**: Inserire la Maschera Subnet WAN qui.
- **Gateway**: Inserire il Gateway WAN qui.
- **Server DNS primario**: Inserire il server primario DNS fornito dal vostro ISP.
- **Server DNS primario**: Inserire il DNS secondario.

Capitolo 6: Impostazioni Wireless

6.1 Impostazioni di Base

- **Abilitare il Wireless**: Selezionare per abilitare il wireless del Router; deselezionare per disabilitarlo.
- **Modalità di Rete**: Selezionare una modalità dalle seguenti. Quella predefinita è la modalità 11b/g/n

- **SSID Principale**: Il SSID (Service Set Identifier) è l'unico nome della rete wireless. Questo dispositivo possiede due SSID e l'SSID principale è necessario.
- **SSID minore**: Questo è opzionale.
- **Trasmissione (SSID)**: Selezionare “abilita” per abilitare l'SSID del dispositivo per essere visibile ai clienti wireless. Come predefinito sarà abilitato.
- **Isolamento AP MBSSID**: Una caratteristica di controllo accesso basato sull'indirizzo MAC wireless. Quando questa caratteristica è attivata, i clienti wireless connessi con lo stesso SSID non possono comunicare tra loro.
- **Isolamento AP**: Una caratteristica di controllo accesso basata sull'SSID. Quando questa funzione è attivata, ciascuno dei vostri clienti wireless rimarrà nella propria rete virtuale e non potrà comunicare con gli altri. Quando questa funzione è attivata, i clienti wireless connessi all'SSID principale e all'SSID minore non potranno comunicare tra di loro, il che porrà in forte sicurezza la rete wireless.
- **Canale**: Specificare il canale effettivo (da 1 a 13\Auto) della rete wireless.
- **Estensione Canale**: Per aumentare i dati attraverso la rete wireless, il range di estensione canale è utilizzato in modalità 11n.
- **Banda Canale**: Selezionare la banda canale per migliorare la prestazione della wireless. Quando la rete ha clienti 11b/g e 11n, potete selezionare i 40M; quando la rete è una rete 11n, selezionare 20/40M per migliorare il proprio trasferimento.

6.2 Impostazioni di sicurezza Wireless

Sono utilizzate per configurare le impostazioni di sicurezza della rete AP. Qui i sei modi più comuni (in genere ve ne sono 10) di codifica, inclusi la WEP mista, la WPA personale, la WPA aziendale, WPA2 personale, WPA2 aziendale ecc.

6.2.1 WEP Mista

WEP (Privacy Equivalente al via cavo), un metodo base di codifica, che generalmente codifica i dati wireless usando una serie di chiavi digitali (64bit o 128 bit in lunghezza). Utilizzando le stesse chiavi su ogni dispositivo delle vostra rete wireless, potete evitare che dispositivi wireless non autorizzati possano monitorare le vostre trasmissioni o usare le vostre risorse di rete wireless. Selezionare WEP mista per accedere alla seguente finestra:

- **Selezionare l'SSID**: Selezionare l'SSID (principale o minore) per configurare le impostazioni di sicurezza dal menu a tendina.
- **Modalità di sicurezza**: Dal menu a tendina, selezionare i modi di codifica di sicurezza corrispondenti.
- **Chiave WEP 1~4**: Impostare la chiave WEP con ASCII e formato Hex. Potete inserire codice ASCII (5 o 13 caratteri ASCII. Caratteri illegali come “/” non sono permessi). o caratteri hex 10/26.
- **Chiave predefinita**: Selezionare una chiave dalle 4 chiavi configurate come quella attualmente disponibile.

6.2.2 WPA- Personale

WPA (Accesso Wi-Fi Protetto), uno standard Wi-Fi, è uno schema di codifica wireless più recente, progettato per migliorare la sicurezza dei dati della WEP. Applica tipi di codifica più potenti (come il TKIP [Protocollo di Integrità Chiave Temporale] o AES [Standard di codifica avanzato]) e può cambiare le chiavi in modo dinamico ad ogni dispositivo wireless autorizzato.

- **Selezionare l'SSID**: Selezionare l'SSID (principale o minore) per configurare le impostazioni di sicurezza dal menu a tendina.
- **Algoritmi WPA**: Fornisce TKIP [Protocollo di Integrità Chiave Temporale] o AES [Standard di codifica avanzato]. Quello predefinito è il modo TKIP.
- **Frase di accesso**: Inserire i caratteri codificati con 8-63 caratteri ASCII.

- **Intervallo di rinnovo chiave**: Impostare il periodo di rinnovo della chiave.

6.2.3 WPA2- Personale

WPA2 (WPA Accesso Wi-Fi Protetto versione 2) fornisce sicurezza maggiore rispetto a WEP (Privacy Equivalente al via cavo), e WPA (Accesso Wi-Fi Protetto)

- **Selezionare l'SSID**: Selezionare l'SSID (principale o minore) per configurare le impostazioni di sicurezza dal menu a tendina.
- **Algoritmi WPA**: Fornisce TKIP [Protocollo di Integrità Chiave Temporale] o AES [Standard di codifica avanzato]. Quello predefinito è il modo TKIP.
- **Frase di accesso**: Inserire i caratteri codificati con 8-63 caratteri ASCII.
- **Intervallo di rinnovo chiave**: Impostare il periodo di rinnovo della chiave.

6.2.4 WPA- Aziendale

Questa modalità di sicurezza è utilizzata quando è connesso un server RADIUS* al dispositivo. Selezionare "WPA- Azienda" dal menu a tendina per accedere alla seguente finestra:

* **RADIUS** (Remote Authentication Dial-In User Service)

- **Selezionare l'SSID**: Selezionare l'SSID (principale o minore) per configurare le impostazioni di sicurezza dal menu a tendina.
- **Algoritmo WPA**: Fornisce TKIP [Protocollo di Integrità Chiave Temporale] o AES [Standard di codifica avanzato]. Quello predefinito è il modo TKIP.
- **Intervallo di rinnovo chiave**: Impostare il periodo di rinnovo della chiave.
- **Server Radius**: Inserire l'indirizzo IP del server Radius.
- **Porta Server Radius**: Inserire la porta di autenticazione del server Radius. Quella predefinita è 1812.
- **Segreto Condiviso**: Inserire una chiave condivisa per il server di autenticazione con 8-63 caratteri ASCII.
- **Tempo limite Sessione**: Il periodo di intervallo di autenticazione tra l'AP ed il server di autenticazione.

6.2.5 WPA2-Azienda

Questo metodo di sicurezza è basato su server di autenticazione a Radius e metodo di codifica WPA2. La WPA2 è utilizzata quando è connesso un server RADIUS al dispositivo. Selezionare "WPA2- Azienda" dal menu a tendina per accedere alla seguente finestra:

- **Selezionare l'SSID**: Selezionare l'SSID (principale o minore) per configurare le impostazioni di sicurezza dal menu a tendina.
- **Algoritmi WPA**: Fornisce TKIP [Protocollo di Integrità Chiave Temporale] o AES [Standard di codifica avanzato]. Quello predefinito è il modo TKIP.
- **Intervallo di rinnovo chiave**: Impostare il periodo di rinnovo della chiave.
- **Server Radius**: Inserire l'indirizzo IP del server Radius.
- **Porta Server Radius**: Inserire la porta di autenticazione del server Radius. Quella predefinita è 1812.
- **Segreto Condiviso**: Inserire una chiave condivisa per il server di autenticazione con 8-63 caratteri ASCII.
- **Tempo limite Sessione**: Il periodo di intervallo di autenticazione tra l'AP ed il server di autenticazione. Come predefinito è 3600s

6.2.6 802.1X

Questa modalità di sicurezza è utilizzata quando è connesso un server RADIUS al dispositivo. 802.1x, un tipo di protocollo di autenticazione basato su porta, una tipo di autenticazione e strategia per utenti. La porta può essere sia fisica che logica (come una VLAN). Per gli utenti di LAN wireless, una porta è solo un canale. Lo scopo finale dell'autenticazione 802.11x è di controllare se la porta può essere usata. Se la porta è autenticata con successo, potete aprire questa porta che vi permette il passaggio di tutti i messaggi. Se la porta non è autenticata con successo, potete mantenere questa porta disabilitata che permette solo il passaggio dei soli messaggi di protocollo di autenticazione "802.1x". Selezionare "802.1x" dal menu a tendina per accedere alla seguente finestra:

- **Selezionare l'SSID**: Selezionare l'SSID (principale o minore) per configurare le impostazioni di sicurezza dal menu a tendina.
- **WEP**: Cliccare "abilita/disabilita" per abilitare o disabilitare l'algoritmo WEP.
- **Server Radius**: Inserire l'indirizzo IP del server Radius.
- **Porta Server Radius**: Inserire la porta di autenticazione del server Radius. Quella predefinita è 1812.
- **Segreto Condiviso**: Inserire una chiave condivisa per il server di autenticazione con 8-63 caratteri ASCII.
- **Tempo limite Sessione**: Il periodo di intervallo di autenticazione tra l'AP ed il server di autenticazione. Come predefinito è 3600s

6.4 Impostazioni WPS

WPS (Impostazione Protetta Wi-Fi) può essere usato facilmente e velocemente per stabilire una connessione tra i clienti di rete wireless ed il dispositivo attraverso contenuti codificati. Gli utenti inseriscono semplicemente un codice PIN o premono il pulsante WPS sul pannello per configurarlo senza dover selezionare manualmente un metodo di codifica e chiavi segrete. Nel menu di "impostazioni wireless", cliccare su "impostazioni WPS" per accedere alla schermata successiva.

- **Impostazioni WPS**: Per abilitare o disabilitare la funzione WPS. Come predefinito sarà "disabilitato".
- **Modalità WPS**: Fornisce due vie: PBC (Configurazione a pulsante) e codice PIN.
- **PBC**: Selezionare il PBC o premere il pulsante WPS sul pannello frontale del dispositivo per circa un secondo (premere il pulsante per circa un secondo e l'indicatore WPS lampeggerà per 2 minuti, che significa che il WPS è abilitato. Mentre sta lampeggiando, potete abilitare un altro dispositivo per completare la negoziazione WPS/PBC tra di essi. Dopo due minuti, l'indicatore WPS si spegnerà, che significa che la connessione WPS è completata. Se più clienti sono aggiunti, ripetete i passi di cui sopra. Al presente, il WPS supporta l'accesso di fino a 32 clienti.)
- PIN: Se viene attivata questa opzione, dovrete inserire un PIN cliente wireless nel campo relativo e inserire lo stesso codice nel cliente WPS.

6.5 Impostazioni WDS

Il WDS (Sistema di distribuzione wireless) è utilizzato per espandere l'area di copertura wireless. Questo Router vi fornisce tre modalità: Pigro, Ponte e Ripetitore.

Pigro: In questa modalità, il dispositivo connesso può essere in modalità Ponte o Ripetitore e inserite il BSSID del Router per stabilire la connessione.

Ponte: Potete connettere wireless due o più reti via cavo attraverso questa modalità. In questa modalità necessitate di aggiungere un indirizzo MAC wireless dei dispositivi in connessione nella tavola di indirizzi MAC AP del Router o selezionarne uno dalla tavola di scansione.

Modalità Ripetitore: In questa modalità aggiungete un indirizzo MAC oppositore in ogni tavola di indirizzi MAC AP relativi manualmente o attraverso lo scanner per allargare o estendere la radio wireless.

Capitolo 7: Server DHCP

7.1 Impostazioni DHCP

Il DHCP (Protocollo di controllo host dinamico) assegna un indirizzo IP ai computer sulla rete LAN/privata. Quando attivate il server DHCP, esso allocherà automaticamente un indirizzo IP non utilizzato dalla serie di indirizzi IP al computer che lo richiede al momento dell'attivazione "Ottieni un indirizzo IP automaticamente". Quindi specificare l'inizio e la fine dell'indirizzo della serie degli indirizzi IP è necessario.

- **Server DHCP**: Attivare la selezione per abilitare il server DHCP.
- **Avvio/fine Indirizzo IP**: Inserire un range degli indirizzi IP per la distribuzione del server DHCP.
- **Tempo di prestito**: La lunghezza del prestito dell'indirizzo IP.

Capitolo 8: Aggiornamento del Firmware

8.1. Il router fornisce un aggiornamento del firmware cliccando “Aggiorna” dopo aver sfogliato il pacchetto di aggiornamento firmware che potete scaricare da www.nedis.nl.

- **Sfogliare**: cliccare questo pulsante per selezionare il file di aggiornamento.
- **Aggiorna**: cliccare questo pulsante per iniziare il processo di aggiornamento. Dopo che l'aggiornamento è completato il Router si riavvierà automaticamente.

8.2 Riavvio del Router

Il Riavvio del Router renderà effettive le impostazioni configurate o imposta nuovamente il Router se le impostazioni non hanno avuto successo.

8.3 Modificare la password

Questa sezione è per impostare un nuovo nome utente e password per assicurare in modo migliore il vostro router e rete.

- **Nome Utente**: Inserire un nuovo nome utente per il dispositivo.
- **Vecchia Password**: Inserire la vecchia password.
- **Nuova Password**: Inserire una nuova password.
- **Re-inserirla per Confermare**: Re-inserire per confermare la nuova password.

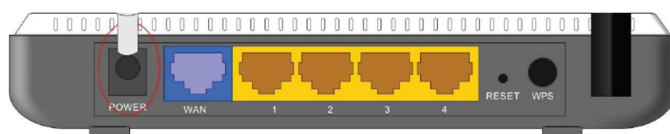
8.4 Uscita

Dopo che avete ultimato tutte le impostazioni, cliccate su “si” sulla pagina di uscita per uscire dalla pagina di gestione web

Come installare ed impostare un router su di un modem via cavo o ADSL

Precauzione!
Seguire questi passi senza saltarne nemmeno uno

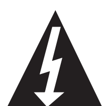
1 Spegnere il modem (disconnetterlo dall'alimentazione).
2. Spegnere PC/Laptop.
3. Collegare **l'uscita LAN** del modem attraverso il **cavo LAN** alla **porta blu** del router.
4. Collegare una delle **porte gialle** attraverso il **cavo LAN** al PC/laptop.



5 Ora accendere il modem ed attendere fino a che abbia fatto l'accesso completo (ciò potrebbe richiedere un momento).
6 Accendere il router ed attendere almeno 30 secondi.
7 Avviare il PC/Laptop ed attendere fino a che si sia avviato totalmente.
8. Aprire il vostro browser e navigare su http://192.168.0.1.
9. Inserire il nome utente e la password (entrambi predefiniti come: **admin**).
10 Navigare su **Setup Wizzard** e cliccare su **Auto Detect**.
11. Ora cliccare su **Avanti** e nelle schermata successiva cliccare su **Applica**.
12. Navigare sul meno di **impostazioni WLAN** ed assicurarsi che sia selezionato **Abilita Wireless** .
13 Qui potete configurare il vostro nome di rete (SSID) ed il canale.
14. Navigate sul sotto menu **Impostazioni di Sicurezza** e selezionate il tipo di sicurezza. Vi raccomandiamo di selezionare sempre **Misto WPA/WPA2 - Personale**.

15. Selezionare **Algoritmo WPA** come **TKIP&AES**.
16. Cambiare la password nel campo **Frase d'accesso**. Raccomandiamo che si selezioni una password forte consistente di lettere, numeri e possibilmente anche almeno 1 carattere speciale.
17. Cliccare su **Applica** per salvare i dati.
18 Uscire dalla schermata browser; la vostra rete senza fili e le impostazioni di sicurezza sono completate. In via opzionale potete disconnettere il cavo tra il router ed il PC/Laptop per gestire solo la connessione wireless (se il PC/laptop è dotato di un ricevitore wireless).

Precauzioni di sicurezza:






Per ridurre il rischio di shock elettrico, questo prodotto dovrebbe essere aperto SOLO da un tecnico autorizzato quando è necessario ripararlo. Scollegare il prodotto dall'alimentazione e da altri apparecchi se dovesse esserci un problema. Non esporre il prodotto ad acqua o umidità.

Manutenzione:

Pulire solo con un panno asciutto. Non utilizzare solventi detergenti o abrasivi.

Garanzia:

Non sarà accettata alcuna garanzia o responsabilità in relazione a cambiamenti e modifiche del prodotto o a danni determinati dall'uso non corretto del prodotto stesso.

Generalità:

- Il design e le caratteristiche tecniche sono soggetti a modifica senza necessità di preavviso.
- Tutti i marchi a logo e i nomi di prodotto sono marchi commerciali o registrati dei rispettivi titolari e sono riconosciuti come tali in questo documento.
- Questo manuale è stato redatto con cura. Tuttavia da esse non possono essere avanzati diritti. König Electronic non può accettare responsabilità per errori in questo manuale nè per eventuali conseguenze.
- Tenere questo manuale e la confezione per riferimento futuro.

Attenzione:



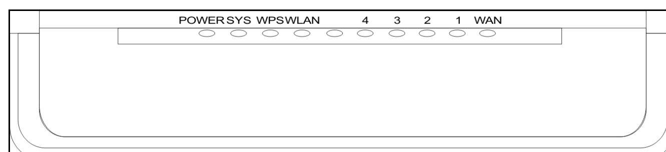
Il prodotto è contrassegnato con questo simbolo, con il quale si indica che i prodotti elettrici ed elettronici non devono essere gettati insieme ai rifiuti domestici. Per questi prodotti esiste un sistema di raccolta differenziata.

ESPAÑOL

Capítulo 1: introducción

1.1 Indicador LED y descripción de puertos

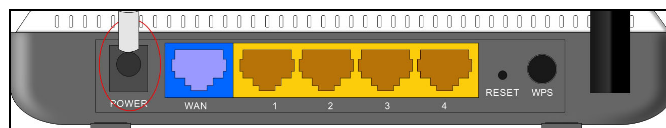
Panel frontal y pantalla del indicador LED



Descripción del indicador LED en el panel frontal: **(de I a D)**

- **POWER (ALIMENTACIÓN)**
  Cuando la luz verde permanece encendida, indica que la alimentación está conectada adecuadamente.
- **SYS**
  Cuando la luz verde parpadea, indica que el sistema funciona correctamente.
- **WPS**
  Cuando parpadea indica que el dispositivo está negociando con el cliente en modo WPS.
- **WLAN**
  Indicador LED de señal inalámbrica. Cuando la luz verde parpadea, indica que la función inalámbrica está activada.
- **LAN (4, 3, 2, 1)**
  Indicador LED de red local con cables. Si permanece encendido, indica que está conectado al dispositivo Ethernet; si parpadea indica que el dispositivo está transmitiendo y/o recibiendo datos.
- **WAN**
  Indicador de red de área de banda ancha. Si permanece encendido indica la banda ancha del router.

Imagen del panel posterior:



Panel posterior: (De I a D)

- **POWER (ALIMENTACIÓN)**

La entrada es para la conexión del adaptador de alimentación. Rogamos use el adaptador de alimentación de CC de 9V que se adjunta.

- **WAN**

Un puerto Ethernet de 100Mbps que puede conectarse con un MÓDEM, Conmutador, Router y otros dispositivos Ethernet para la conexión a Internet mediante MÓDEM ADSL, MÓDEM PARA CABLE e ISP.

- **LAN (1, 2, 3, 4)**

4 puertos Ethernet de 10/100Mbps que pueden conectarse con un conmutador Ethernet, un router Ethernet y una tarjeta NIC.

- **RESET (REINICIO)**

El botón de reinicio del sistema. Pulse este botón durante 7 segundos; se borrarán los ajustes configurados en este dispositivo y se restaurará la configuración por defecto.

- **WPS**

Púlselo durante 1 segundo; se activará la propiedad WPS y parpadeará el indicador WPS.

Capítulo 2: Instalación del hardware

2.1 Cómo instalar el router

Por favor, utilice el adaptador de alimentación que se adjunta para alimentar su router. IMPORTANTE: El uso de un adaptador de alimentación diferente puede provocar daños y anular la garantía de este producto. Por favor, conecte el puerto LAN del router al adaptador de red de su ordenador utilizando un cable. Por favor, conecte su línea de banda ancha suministrada por su ISP al puerto WAN. Inserte el CD-ROM adjunto en la unidad de CD-ROM; haga doble clic en el icono "Setup (Instalación)" y siga las instrucciones para completar la instalación. O puede entrar el la página Web del router para configurarlo. (Para obtener más detalles, por favor, remítase al Capítulo 3.)

Capítulo 3: Cómo iniciar sesión con el router

3.1 Cómo establecer las configuraciones de red

1. En el escritorio de su ordenador, haga clic en "Mis sitios de red" y seleccione "Propiedades".
2. Haga clic en "Conexión de Red de Área Local" y seleccione "Propiedades".
3. Seleccione "Protocolo de Internet (TCP/IP)" y haga clic en "Propiedades".
4. - Seleccione "Obtener una dirección IP automáticamente" y "Obtener dirección del servidor DNS automáticamente". Haga clic en "OK" para guardar la configuración.
   - O seleccione "Usar la siguiente dirección IP" e introduzca la dirección IP, mascara Subnet y vía predeterminada de la manera siguiente: Dirección IP: 192.168.0.XXX: (XXX es un número del 2~254) Máscara Subnet: 255.255.255.0.
     Vía: 192.168.0.1. Es absolutamente necesario que introduzca la dirección del servidor DNS que suministra la ISP. En caso contrario, puede usar la vía predeterminada del router como servidor proxy DNS. Haga clic en "OK" para guardar la configuración.

3.2 Inicio de sesión en el router

1. Para acceder a la interfaz basada en Web del router, lance un buscador de páginas Web como, por ejemplo, Internet Explorer o Firefox e introduzca la dirección IP por defecto del router, http://192.168.0.1. Pulse "Intro".
2. Introduzca "admin" tanto como nombre de usuario como contraseña. Haga clic en "OK".

Configuración por defecto	
Dirección IP	192.168.0.1
Contraseña	admin
SSID	KONIG
Modo de seguridad	Desactivado
Modo inalámbrico	Modo b/g/n Mixd
Canal	Selección automática
Zona horaria	
Configuración WPS	Activada
Nombre del dispositivo UPNP	Router inalámbrico de banda ancha 11N
Fabricante UPNP	KONIGELECTRONIC
Nombre / Modelo UPNP	CMP-WNROUT41
Número de modelo UPNP	V 1.0
Velocidad de red reportada UPNP	300Mbps
Dirección del dispositivo UPNP	http://192.168.0.1
UPNP	Desactivado

Capítulo 4: Guía de instalación rápida

4.1 Asistente de instalación

Aquí nos encontramos “Bienvenido al asistente de instalación” para conseguir una instalación rápida de su router. Haga clic en “Siguiente”.

En esta pantalla, seleccione un modo de conexión a Internet que emplee. Si no está seguro, pulse el botón “Detectar” o póngase en contacto con su proveedor de servicios de Internet y haga clic en “Siguiente”.

Marcación virtual por ADSL (Vía PPPoE)

Introduzca la cuenta y la contraseña proporcionada por su ISP, y haga clic en “Siguiente”.

IP dinámica (Vía DHCP)

Si su modo de conexión es una IP dinámica, indica que su dirección IP cambia cada vez que se conecta. No es necesario que introduzca la información como en otros modos. Haga clic en “Siguiente” y “Guardar” para finalizar la configuración.

IP estática

En esta pantalla, introduzca la información en los campos del servidor de su dirección de red de su ISP en Dirección IP, Máscara Subnet, Vía y DNS primaria y haga clic en “Siguiente”.

L2TP

Consulte a su ISP para obtener la información necesaria.

Capítulo 5: Configuración avanzada

5.1 Configuración LAN

La configuración LAN se emplea para los parámetros básicos de TCP/IP de los puertos LAN.

- **Dirección IP**: Las direcciones IP LAN del router (no la dirección IP de su PC). 192.168.0.1 es el valor por defecto.
- **Máscara Subnet**: Muestra la mascara Subnet del router para medir el tamaño de la red. 255.255.255.0 es el valor por defecto.

IMPORTANTE:

Una vez que modifique la dirección IP, es necesario que la recuerde para el próximo inicio de sesión en la utilidad basada en Web.

5.2 Configuración WAN

Una vez que haya seleccionado el tipo de conexión ISP en el “Asistente de instalación” y desee modificar la configuración relacionada, puede modificar y configurar los ajustes al detalle aquí.

IP estática

Si se elige como modo de conexión una IP estática, puede modificar la siguiente información de la dirección.

- **Dirección IP**: Introduzca aquí la dirección IP WAN suministrada por su ISP.
- **Máscara Subnet**: Introduzca aquí la Máscara Subnet WAN.
- **Vía**: Introduzca aquí la Vía WAN.
- **DNS primaria del servidor**: Introduzca aquí la DNS primaria del servidor proporcionada por su ISP.
- **DNS secundaria del servidor**: Introduzca aquí la DNS secundaria.

Capítulo 6: Configuración inalámbrica

6.1 Configuración básica

- **Activar inalámbrico**: Márquelo para activar las propiedades inalámbricas del router; no lo marque para desactivarlas.
- **Modo de red**: Seleccione un modo entre los siguientes. El modo por defecto es 11b/g/n.

- **SSID principal**: El SSID (Identificador de conjuntos de servicios) es el único nombre de la red inalámbrica. Este dispositivo dispone de dos SSID y el SSID es necesario.
- **SSIB menor**: Éste es opcional.
- **Emisión (SSID)**: Seleccione “Activar” para activar el SSID del dispositivo de forma que esté visible para los clientes inalámbricos. Por defecto, se encuentra activado.
- **Aislamiento MBSSID AP**: Una propiedad de control de acceso basada en la dirección inalámbrica MAC. Cuando esta propiedad está activada, los clientes inalámbricos conectados al mismo SSID no se pueden comunicar entre si.
- **Aislamiento AP**: Una propiedad de control de acceso basada en SSID. Cuando esta propiedad está activada, cada uno de los clientes inalámbricos estarán en su propia red virtual y no podrán comunicarse entre si. Cuando esta propiedad está activada, los clientes inalámbricos conectados al SSID principal y al SSID menor no pueden comunicarse entre si, lo que puede asegurar enormemente la red inalámbrica.
- **Canal**: Especifique el canal efectivo (del 1 al 13\Auto) de la red inalámbrica.
- **Canal de extensión**: para aumentar la tasa de transferencia de datos de la red inalámbrica, el ámbito del canal de extensión se usa en modo 11n.
- **Anchura de banda del canal**: Seleccione la anchura de banda del canal para mejorar el rendimiento inalámbrico. Cuando la red presenta 11b/g y 11n clientes, puede seleccionar el 40M; cuando se trata de una red 11n, seleccione 20/40M para mejorar la tasa de transferencia.

6.2 Configuración de seguridad inalámbrica

Esto se emplea para configurar los ajustes de seguridad de red de AP. Aquí se presentan los seis métodos de encriptación más comunes (diez en total), incluyendo WEP mixta, WPA personal, WPA empresa, WPA2 personal, WPA2 empresa, etc.

6.2.1 WEP mixta

WEP (Privacidad equivalente por cable), es un método de encriptación básico que normalmente encripta datos inalámbricos usando una serie de claves digitales (64 bits o 128 bits de longitud). Al usar las mismas claves en cada uno de sus dispositivos de red inalámbricos, puede evitar que los dispositivos inalámbricos no autorizados monitoricen sus transmisiones o empleen sus recursos inalámbricos. Seleccione WEP mixta para entrar en la ventana siguiente:

- **Seleccionar SSID**: Seleccione la SSID (SSID principal o SSID menor) para configurar los ajustes de seguridad desde el menú desplegable.
- **Modo de seguridad**: Desde el menú desplegable, seleccione los modos de encriptación de seguridad correspondientes.
- **WEP Clave 1~4**: Establezca la clave WEP con el formato ASCII y Hexadecimal. Puede introducir el código ASCII (5 o 13 caracteres ASCII; no se permiten los caracteres ilegales como “/”.) o caracteres 10/26 hexadecimales.
- **Clave por defecto**: Seleccione una clave de las cuatro claves configuradas como la actual disponible.

6.2.2 WPA Personal

WPA (Acceso Protegido Wi-Fi), un estándar Wi-Fi, es un plan de encriptación inalámbrica muy reciente, diseñado para mejorar las propiedades de seguridad de WEP. Aplica tipos de encriptación más potentes (como TKIP [Protocolo de Integridad de Clave Temporal] o AES [Estándar de Encriptación Avanzada]) y puede cambiar las claves de forma dinámica en cada dispositivo inalámbrico autorizado.

- **Seleccionar SSID**: Seleccione la SSID (SSID principal y SSID menor) para configurar los ajustes de seguridad desde el menú desplegable.
- **Algoritmos WPA**: Ofrece TKIP [Protocolo de Integridad de Clave Temporal] o AES [Estándar de Encriptación Avanzada]. El modo por defecto es TKIP.
- **PassPhrase**: Introduzca los caracteres encriptados con caracteres 8-63 ASCII.

- **Intervalo de renovación de clave**: Establezca el periodo de renovación de clave.

6.2.3 WPA2 Personal

WPA2 (Acceso Protegido Wi-Fi versión 2) ofrece una mayor seguridad que WEP (Privacidad Equivalente Inalámbrica) y WPA (Acceso Protegido Wi-Fi).

- **Seleccionar SSID**: Seleccione la SSID (SSID principal y SSID menor) para configurar los ajustes de seguridad desde el menú desplegable.
- **Algoritmos WPA**: Ofrece TKIP [Protocolo de Integridad de Clave Temporal] o AES [Estándar de Encriptación Avanzada]. El modo por defecto es TKIP.
- **PassPhrase**: Introduzca los caracteres encriptados con caracteres 8-63 ASCII.
- **Intervalo de renovación de clave**: Establezca el periodo de renovación de clave.

6.2.4 WPA Empresa

Este modo de seguridad se emplea cuando un servidor RADIUS se conecta al dispositivo. Seleccione “WPA-Enterprise” del menú desplegable para entrar en la ventana siguiente:

- **Seleccionar SSID**：Seleccione la SSID (SSID principal y SSID menor) para configurar los ajustes de seguridad desde el menú desplegable.
- **Algoritmos WPA**：Ofrece TKIP [Protocolo de Integridad de Clave Temporal] o AES [Estándar de Encriptación Avanzada]. El modo por defecto es TKIP.
- **Intervalo de renovación de clave**: Establezca el periodo de renovación de clave.
- **Servidor Radius**: Introduzca la dirección IP del servidor Radius.
- **Puerto del servidor Radius**: Introduzca el puerto de autenticación del servidor Radius. El puerto por defecto es 1812.
- **Secreto compartido**: Introduzca la clave compartida para el servidor del autenticación con 8~63 caracteres ASCII.
- **Desconexión de sesión por tiempo**: El periodo de intervalo de autenticación entre AP y el servidor de autenticación.

6.2.5 WPA2 Empresa

Este modo de seguridad se basa en el servidor de autenticación Radius y el método de encriptación WPA2. El WPA2 se usa cuando un servidor RADIUS se conecta al dispositivo. Seleccione “WPA2-Enterprise” desde el menú desplegable para entrar en la ventana siguiente:

- **Seleccionar SSID**：Seleccione la SSID (SSID principal y SSID menor) para configurar los ajustes de seguridad desde el menú desplegable.
- **Algoritmos WPA**：Ofrece TKIP [Protocolo de Integridad de Clave Temporal] o AES [Estándar de Encriptación Avanzada]. El modo por defecto es TKIP.
- **Intervalo de renovación de clave**: Establezca el periodo de renovación de clave.
- **Servidor Radius**: Introduzca la dirección IP del servidor Radius.
- **Puerto del servidor Radius**: Introduzca el puerto de autenticación del servidor Radius. El puerto por defecto es 1812.
- **Secreto compartido**: Introduzca la clave compartida para el servidor del autenticación con 8~63 caracteres ASCII.
- **Desconexión de sesión por tiempo**: El periodo de intervalo de autenticación entre AP y el servidor de autenticación. El periodo por defecto es de 3600s.

6.2.6 802.1X

Este modo de seguridad se usa cuando un servidor RADIUS se conecta al dispositivo. 802.1x, es un tipo de protocolo y estrategia de autenticación basado en puerto para usuarios. El puerto puede ser bien un puerto físico o un puerto lógico (como VLAN). Para usuarios LAN inalámbricos, un puerto es simplemente un canal. El objetivo final de la autenticación 802.11x es comprobar si se puede usar el puerto. Si el puerto se autentica

con éxito, puede abrir este puerto lo que permite que pasen todos los mensajes. Si el puerto no se autentica con éxito, puede mantener este puerto “desactivado” lo que solo permiten que pasen los mensajes del protocolo de autenticación 802.1x. Seleccione “802.1x” desde el menú desplegable para entrar en la ventana siguiente:

- **Seleccionar SSID**： Seleccione la SSID (SSID principal y SSID menor) para configurar los ajustes de seguridad desde el menú desplegable.
- **WEP**: Haga clic en “Activar/Desactivar” para activar o desactivar el algoritmo WEP.
- **Servidor Radius**: Introduzca la dirección IP del servidor Radius.
- **Puerto del servidor Radius**: Introduzca el puerto de autenticación del servidor Radius. El puerto por defecto es 1812.
- **Secreto compartido**: Introduzca la clave compartida para el servidor del autenticación con 8~63 caracteres ASCII.
- **Desconexión de sesión por tiempo**: El periodo de intervalo de autenticación entre AP y el servidor de autenticación. El periodo por defecto es de 3600s.

6.4 Configuración WPS

La WPS (Configuración Wi-Fi Protegida) puede usarse para establecer de forma rápida y fácil la conexión entre los clientes de la red inalámbrica y el dispositivo mediante contenidos encriptados. Los usuarios solo introducen un código PIN o pulsan el botón WPS del panel para configurarlo son seleccionar manualmente la selección de un método de encriptación y de claves secretas. En el menú “Configuración inalámbrica” haga clic en “Configuración WPS” para entrar en la ventana siguiente.

- **Configuración WPS**: Para activar o desactivar la función WPS. La función por defecto es “desactivada”.
- **Modo WPS**: Ofrece dos formas: PBC (Configuración mediante botón) y código PIN.
- **PBC**: Seleccione el PBC o pulse el botón WPS en el panel frontal del dispositivo durante aproximadamente un segundo (Pulse el botón durante aproximadamente un segundo y el indicador WPS parpadeará durante 2 minutos, lo que indica que el WPS está activado. Mientras parpadea, puede activar otro dispositivo para implementar la negociación WPS/PBC entre ellos. Después de dos minutos, el indicador WPS se apaga, lo que indica que se ha completado la conexión WPS. Si se añaden más clientes, repita los pasos que se describen arriba. En este momento, el WPS es compatible con el acceso de hasta 32 clientes.)
- PIN: Si se active esta opción, es necesario que introduzca un código PIN de cliente inalámbrico en el campo y mantener el mismo código con el cliente WPS.

6.5 Configuración WDS

El WDS (Sistema de Distribución Inalámbrico) se usa para aumentar el área de cobertura inalámbrica. Este router ofrece tres modos: Perezoso, Bridge y Repetidor.

Perezoso: En este modo, el dispositivo conectado puede estar bien en modo Bridge o en modo Repetidor, e introducir la BSSID del router para establecer la conexión.

Bridge: Puede conectar de forma inalámbrica dos o más redes de cable mediante este modo. En este modo, es necesario que se añada la dirección MAC inalámbrica del dispositivo que se conecta en la tabla de dirección MAC AP del router o seleccionar uno de la tabla de búsqueda.

Modo repetidor: En este modo, añada la dirección MAC contraria en cada tabla de dirección propia AP MAC de forma manual o mediante escáner para alargar y aumentar la radio inalámbrica.

Capítulo 7: Servidor DHCP

7.1 Configuración DHCP

El DHCP (Protocolo de Control Dinámico de Host) asigna una dirección IP a los ordenadores de la red LAN / privada. Al activar el Servidor DHCP, el Servidor DHCP adjudicará de forma automática una dirección IP sin usar del conjunto de direcciones IP al ordenador que lo solicite bajo la premisa de activar “Obtener una

dirección P automáticamente”. Por los tanto, es necesario la dirección de inicio y fin del conjunto de direcciones IP.

- **Servidor DHCP**: Active la casilla para activar el servidor DHCP.
- **Inicio / Fin de dirección IP**: Introduzca el ámbito de la dirección IP para la distribución del servidor DHCP.
- **Tiempo de arrendamiento**: La duración del arrendamiento de la dirección IP.

Capítulo 8: Actualizar el firmware

8.1 El router ofrece una actualización del firmware hacienda clic en “Upgrade (Actualizar)” tras buscar el paquete de actualización de firmware que puede descargar desde la página Web www.nedis.nl

- **Buscar**: haga clic en este botón para seleccionar el archive de actualización.
- **Actualizar**: haga clic en este botón para iniciar el proceso de actualización. Una vez que la actualización está completa, el router se reiniciará de forma automática.

8.2 Reiniciar el router

Reiniciar el router hace que los ajustes de configuración tengan efecto o configure el router de Nuevo si la configuración falla.

8.3 Cambio de contraseña

Esta sección trata de configurar un nuevo nombre de usuario y contraseña para asegurar mejor su router y red.

- **Nombre de usuario**: Introduzca un nuevo nombre de usuario para el dispositivo.
- **Antigua contraseña**: Introduzca la antigua contraseña.
- **Nueva contraseña**: Introduzca una nueva contraseña.
- **Vuelva a introducirla para confirmarla**: Vuelva a introducirla para confirmar la nueva contraseña.

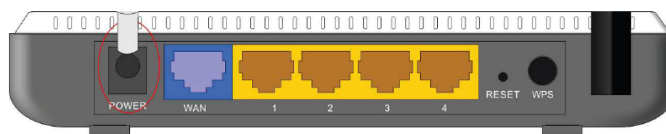
8.4 Fin de sesión

Una vez que haya finalizado completamente la configuración, haga clic en “Sí” en la página de fin de sesión para finalizar sesión en la página de gestión de Webs.

Instalación y configuración de un enrutador con cable o un módem ADSL

¡Precaución!
Por favor, complete estos pasos sin saltearse ninguno

1. Apague el módem (desconéctelo de la toma de electricidad).
2. Apague su PC/portátil.
3. Conecte la salida de **red local (LAN)** del módem a través del **cable de red local** en el **puerto azul** del enrutador.
4. Conecte uno de los **puertos amarillos** a través del **cable de red local** a la Pc/portátil.



5. Encienda el módem y espere a ingresar completamente (esto puede demorar unos momentos).
6. Encienda el enrutador y espere al menos 30 segundos.
7. Encienda su Pc/portátil y espere a que inicie completamente.
8. Inicie su navegador web y diríjase a http://192.168.0.1.
9. Ingrese su nombre de usuario y su contraseña (por defecto ambas son: **admin**).

10. Diríjase al **Asistente de configuración** y haga clic en **Detectar automáticamente**.
11. Ahora haga clic en **Siguiente**, en la pantalla siguiente haga clic en **Aplicar**.
12. Diríjase al menú **Configuración WLAN** y asegúrese de que la opción **Activar wireless** esté seleccionada.
13. Aquí podrá configurar el nombre de su red (SSID) y el canal correspondiente.
14. Diríjase al submenú **Configuraciones de seguridad** y seleccione el tipo de seguridad. Le recomendamos que seleccione **Modo mixto WPA/WPA 2 — Personal.**
15. Seleccione los **algoritmos WPA** como **TKIP&AES**.
16. Cambie la contraseña en el campo **Frase de contraseña**. Le recomendamos elegir una contraseña robusta, que consista de letras, números y en lo posible uno o más caracteres especiales.
17. Haga clic en **Aplicar** la guardar los cambios.
18. Salga de la pantalla del navegador. A partir de este momento su red inalámbrica y sus configuraciones estarán listas. Opcionalmente, puede crear una conexión inalámbrica si desconecta el cable entre el enrutador y su PC/portátil (en el caso de que la PC/portátil esté equipada con un receptor inalámbrico).

Medidas de seguridad:



Para reducir el peligro de descarga eléctrica, este producto SÓLO lo debería abrir un técnico autorizado cuando necesite reparación. Desconecte el producto de la toma de corriente y de los otros equipos si ocurriera algún problema. No exponga el producto al agua ni a la humedad.

Mantenimiento:

Límpielo sólo con un paño seco. No utilice disolventes de limpieza ni productos abrasivos.

Garantía:

No se aceptará ninguna garantía o responsabilidad derivada de cualquier cambio o modificaciones realizadas al producto o daños provocados por un uso incorrecto del producto.

General:

- Las ilustraciones y las especificaciones podrán sufrir cambios sin previo aviso.
- Todas las marcas de logotipos y nombres de productos constituyen patentes o marcas registradas a nombre de sus titulares correspondientes, reconocidos como tal.
- Este manual se ha redactado con sumo cuidado. Aún así, no se ofrece ninguna garantía. König Electronic no será responsable de los errores de este manual o de las consecuencias derivadas de los mismos.
- Conserve este manual y el embalaje en caso de futura necesidad.

Atención:



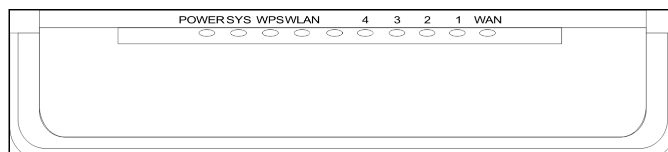
Este producto está señalizado con este símbolo. Esto significa que los productos eléctricos y electrónicos usados no deberán mezclarse con los desechos domésticos generales. Existe un sistema de recogida individual para este tipo de productos.

MAGYAR

1. fejezet: Bevezetés

1.1 LED kijelzők és portok

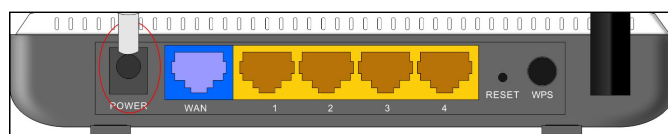
Előlap és LED-ek



Az előlapon levő LED-ek ismertetése: (balról jobbra)

- **POWER (TÁPFESZÜLTSÉG)**
  Ha zölden világít, akkor a készülék kap tápfeszültséget.
- **SYS (RENDSZER)**
  Ha zölden villog, a készülék hibátlanul működik.
- **WPS**
  Ha villog, a készülék WPS módban egyeztet a klienssel.
- **WLAN**
  A vezeték nélküli hálózat működését jelzi. Ha zölden villog, a vezeték nélküli funkció be van kapcsolva.
- **LAN (4, 3, 2, 1)**
  A vezetékes helyi hálózat LED jelzője. Ha világít, a készülék Ethernetes eszközre van kötve; ha villog, a készülék ad és/vagy vesz adatokat.
- **WAN**
  A WAN hálózat jelzője. Ha világít, az útválasztó a WAN hálózatra kapcsolódik.

A hátoldal képe:



A hátoldal: (balról jobbra)

- **POWER (TÁPFESZÜLTSÉG)**

A tápfeszültség csatlakozóaljzata. Használja a készülékhez adott 9 V-os hálózati tápegységet.

- **WAN**

100 Mbit/s sebességű Ethernet port. Köthető rá modem, kapcsoló, útválasztó és másik Ethernet eszköz. Az internetszolgáltatóhoz DSL modem és kábelmodem útján csatlakoztatható.

- **LAN (1, 2, 3, 4)**

4 db 10/100 Mbit/s sebességű Ethernet port. Ethernet kapcsolóhoz, Ethernet útválasztóhoz és hálózati kártyához köthető.

- **RESET (VISSZAÁLLÍTÁS)**

Rendszervisszaállító gomb. Ha 7 másodpercig folyamatosan nyomják, a készülék egyéni beállításai törlődnek és visszaállnak a gyári alapbeállításokra.

- **WPS**

Ha 1 másodpercig folyamatosan nyomják, bekapcsolódik a WPS funkció és villogni kezd a WPS LED.

2. fejezet: A hardver üzembehelyezése

2.1 Az útválasztó üzembehelyezése

Kérjük, a készüléket a hozzá adott 9 V-os tápegységgel használja. FONTOS: Más tápegység tönkreteheti a készüléket és érvénytelenítheti jótállását. LAN kábellel kösse össze az útválasztó LAN portját a számítógép hálózati kártyájának csatlakozójával. Csatlakoztassa az internetszolgáltató szélessávú vezetékét a WAN portra. Helyezze a mellékelt CD lemezt a számítógép CD meghajtójába, kattintson duplán a „Setup" (Telepítés) ikonra, és kövesse a megjelenő utasításokat. Az útválasztó weboldalán is elvégezheti a beállítást. (További részletekkel a 3. fejezet szolgál.)

3. fejezet: Bejelentkezés az útválasztóba

3.1 A hálózati konfiguráció beállítása

1. A számítógép asztalán jobb gombbal kattintson a „My Network Places" (Hálózati helyek) ikonra, majd válassza a „Properties" (Tulajdonságok) pontot.
2. Jobb gombbal kattintson a „Local Area Network Connection" (Helyi hálózati kapcsolat) lehetőségre, majd válassza a „Properties" (Tulajdonságok) pontot.
3. Válassza az „Internet Protocol (TCP/IP)" lehetőséget, majd kattintson a „Properties" (Tulajdonságok) pontra.
4. - Válassza az „Obtain an IP address automatically" (IP-cím automatikus kérése) és „Obtain DNS server address automatically" (DNS-kiszolgáló címének automatikus kérése) lehetőséget. Kattintson az „OK" gombra a konfiguráció elmentéséhez.
   - Alternatív megoldásként válassza a „Use the following IP address" (A következő IP-cím használata:) lehetőséget, és adja meg az IP-címet, alhálózati maszkot és alapértelmezett átjárót, a következők szerint: IP Address (IP-cím): 192.168.0.XXX: (ahol XXX egy 2 és 254 közötti szám) Alhálózati maszk: 255.255.255.0.
   Gateway (Átjáró): 192.168.0.1. Be kell írni az internetszolgáltató által megadott DNS kiszolgálócímet is. Ellenkező esetben az útválasztó alapértelmezett átjáróját használhatja DNS proxy kiszolgálóként. Kattintson az „OK" gombra a konfiguráció elmentéséhez.

3.2 Bejelentkezés az útválasztóba

1. Az útválasztó webes felhasználói felületének megnyitásához indítsa el webböngészőjét (Internet Explorer, Firefox, stb.), és írja bele az útválasztó alapértelmezett IP-címét: (http://192.168.0.1.). Nyomjon rá „Enter"-t.
2. A User Name és Password (Felhasználói név és Jelszó) rovatba írja be, hogy „admin" és „admin". Kattintson az „OK" gombra

Alapértelmezett beállítások	
IP address (IP-cím)	192.168.0.1
Password (Jelszó)	admin
SSID	KONIG
Security Mode (Biztonsági mód)	Disable (Letiltva)
Wireless Mode (Vezeték nélküli mód)	b/g/n Mixd Mode
Channel (Csatorna)	Autoselect
Time Zone (Időzóna)	
WPS settings (WPS beállítások)	Enable (Engedélyezve)
UPNP Device Name (UPNP eszköznév)	11N Wireless Broadband Router
UPNP Manufacturer (UPNP gyártó)	KONIGELECTRONIC
UPNP Model Name (UPNP modellnév)	CMP-WNROUT41

UPNP Model Number (UPNP modellszám)	V 1.0
UPNP reported network speed (UPNP jelzett hálózati sebesség)	300Mbps
UPNP Device address (UPNP eszközcím)	http://192.168.0.1
UPNP	Disable (Letiltva)

4. fejezet: Beállítási kisokos

4.1 A beállító varázsló

Ez a beállító varázsló, amellyel gyorsan és könnyen beállíthatja útválasztóját. Kattintson a „Next" (Tovább) gombra.

Ezen a képernyőn jelölje ki internetkapcsolati módját. Ha nem ismeri, kattintson a „Detect" (Észlelés) gombra, vagy forduljon internetszolgáltatójához; kattintson a „Next" (Tovább) gombra.

ADSL Virtual Dial-up (ADSL virtuális betárcsázás PPPoE útján)

Írja be az internetszolgáltatótól kapott Account és Password (azonosító és jelszó) értékét, majd kattintson a „Next" (Tovább) gombra.

Dynamic IP (dinamikus IP-cím, DHCP útján)

Ha Ön dinamikus IP-vel kapcsolódik, akkor minden felkapcsolódáskor más-más IP-címet kap. Itt nem kell megadni értéket, mint más módoknál. Kattintson a „Next" (Tovább) gombra, majd a „Save" (Mentés) gombbal fejezze be a beállítást.

Static IP (statikus IP-cím)

Ezen a képernyőn az IP Address (IP-cím), Subnet Mask (Alhálózati maszk), Gateway (Átjáró) és Primary DNS server (Elsődleges DNS-kiszolgáló) rovatba írja be az internetszolgáltatójától kapott adatokat, majd kattintson a „Next" (Tovább) gombra.

L2TP

Kérdezze meg internetszolgáltatójától, hogy mit írjon ide.

5. fejezet: Speciális beállítások

5.1 LAN beállítások

A LAN beállítások a LAN portok alapvető TCP/IP paramétereire vonatkoznak.

■ IP Address (IP-cím): Az útválasztó LAN IP-címe (tehát nem a számítógép IP-címe). 192.168.0.1 az alapértelmezett érték.

Subnet Mask (alhálózati maszk): Az útválasztónak a hálózatméret mérésére szolgáló alhálózati maszkját mutatja. 255.255.255.0 az alapértelmezett érték.

FONTOS:

Ha módosítja az IP-címet, jegyezze fel értékét, mert szüksége lesz rá a webes segédprogramba való következő belépéshez.

5.2 WAN beállítások

Ha a „Setup Wizard" beállító varázslóban kijelölte az internetszolgáltatóhoz való kapcsolódás típusát, és módosítani szeretné a vonatkozó beállításokat, ezt itt teheti meg.

Static IP (statikus IP-cím)

Ha a kapcsolódás módjaként statikus IP van megadva, módosíthatók a következő címadatok.

■ **IP Address (IP-cím):** Ide kell beírni az internetszolgáltatótól kapott WAN IP-címet.

Subnet Mask (alhálózati maszk): Ide kell beírni a WAN alhálózati maszkértékét.

■ **Gateway (Átjáró):** Ide kell beírni a WAN átjárót.

- **Primary DNS Server (elsődleges DNS-kiszolgáló):** Ide kell beírni az elsődleges DNS-kiszolgáló internetszolgáltatótól kapott adatait.
- **Secondary DNS Server (másodlagos DNS-kiszolgáló):** Ide kell beírni a másodlagos DNS-kiszolgáló adatait.

6. fejezet: Vezeték nélküli beállítások

6.1 Alapbeállítások

- **Enable Wireless (a vezeték nélküli működés engedélyezése):** Ha bejelöli, engedélyezi az útválasztó vezeték nélküli funkcióit. Ha kiveszi a jelölést, e funkciók le lesznek tiltva.
- **Network Mode (hálózati mód):**Válassza a következők egyikét. Az alapértelmezett mód 11b/g/n.
- **Main SSID (fő SSID):**Az SSID (Service Set Identifier) a vezeték nélküli hálózat egyedi azonosítója. Az eszköznek két SSID-je van; a fő SSID-t kötelező megadni.
- **Minor SSID (másodlagos SSID):**Nem kötelező megadni.
- **Broadcast (SSID közzététele):** Az „Enable” kiválasztása esetén az eszköz SSID-jét láthatják a vezeték nélküli ügyfelek. Alapértelmezés szerint láthatják.
- **MBSSID AP Isolation (különválasztás):**A vezeték nélküli MAC-címre épülő hozzáférésvezérlési funkció. Engedélyezett állapotában az azonos SSID-vel csatlakozó vezeték nélküli ügyfelek nem kommunikálhatnak egymással.
- **AP Isolation (különválasztás):** Az SSID-re épülő hozzáférésvezérlési funkció. Engedélyezett állapotában a vezeték nélküli ügyfelek külön-külön saját virtuális hálózatukba vannak bezárva, és nem kommunikálhatnak egymással. Engedélyezett állapotában a fő SSID-vel és a másodlagos SSID-vel kapcsolódó vezeték nélküli ügyfelek nem kommunikálhatnak egymással, ami nagymértékben fokozza a vezeték nélküli hálózat biztonságosságát.
- **Channel (csatorna):** Itt kell megadni a vezeték nélküli hálózat tényleges működési csatornáját, 1 és 13\Auto között.
- **Extension Channel (bővítőcsatorna):**A vezeték nélküli hálózat átviteli kapacitásának növelése végett a bővítőcsatorna tartománya 11n módban működik.
- **Channel Bandwidth (csatorna sávszélesség):**Itt adható meg a csatorna sávszélessége a vezeték nélküli átviteli kapacitás javításához. Ha a hálózatban 11b/g és 11n ügyfelek vannak, válassza a 40M értéket; 11n hálózat esetén válassza a 20/40M értéket az átviteli kapacitás növeléséhez.

6.2 A vezeték nélküli biztonság beállításai

Itt konfigurálhatók az AP hálózat biztonsági beállításai. Itt jelenik meg a leggyakoribb hat (összesen tíz) titkosítási mód, például Mixed WEP (vegyes WEP), WPA-personal, WPA-enterprise, WPA2-personal, WPA2-enterprise, stb.

6.2.1 Mixed WEP (vegyes WEP)

A WEP (Wired Equivalent Privacy) titkosítási alapmódszer rendszerint 64 vagy 128 bit hosszúságú digitális kulcsokkal titkosítja a vezeték nélküli adatokat. A vezeték nélküli hálózat minden eszközén ugyanazon kulcsok használatával megakadályozható, hogy illetéktelenek figyeljék az Ön adatforgalmát vagy használják vezeték nélküli erőforrásait. A Mixed WEP kijelölése esetén a következő ablak jelenik meg:

- **Select SSID (SSID választás):**A legördülő menün kiválaszthatja a fő vagy másodlagos SSID-t a biztonság konfigurálásához.
- **Security Mode (biztonsági mód):**A legördülő menün kiválaszthatja a kívánt titkosítási módot.
- **WEP Key (WEP kulcs), 1–4:**ASCII vagy Hex formátumban adhatja meg a WEP kulcsot. Megadhat ASCII kódot is (5 vagy 13 ASCII karaktert. / és egyéb tiltott karakterek nem használhatók.), vagy 10/26 hexadecimális karaktert.
- **Default Key (alapértelmezett kulcs):**Megadhatja, hogy a négy beállított kulcs közül melyik legyen az aktuális.

6.2.2 WPA-Personal

A WPA (Wi-Fi Protected Access) nevű Wi-Fi szabvány a WEP-nél biztonságosabb vezeték nélküli titkosítási módot ír elő. Maga a titkosítás is teljesítőképesebb (TKIP [Temporal Key Integrity Protocol] vagy AES [Advanced Encryption Standard]), és a WPA dinamikusan tudja módosítani a kulcsokat az engedélyezett vezeték nélküli eszközökön.

- **Select SSID (SSID választás):**A legördülő menün kiválaszthatja a fő vagy másodlagos SSID-t a biztonság konfigurálásához.
- **WPA Algorithms (WPA algoritmus):**TKIP [Temporal Key Integrity Protocol] vagy AES [Advanced Encryption Standard]. A TKIP az alapértelmezett mód.
- **Pass Phrase (kulcskifejezés):**Itt 8-63 ASCII karakterrel adható meg a titkosító kifejezés.
- **Key Renewal Interval (a kulcs megújítási időköze):**Itt állítható be a kulcs megújítási időköze.

6.2.3 WPA2- Personal

A WPA2 (Wi-Fi Protected Access version 2) biztonságosabb, mint a WEP (Wireless Equivalent Privacy) és a WPA (Wi-Fi Protected Access).

- **Select SSID (SSID választás):**A legördülő menün kiválaszthatja a fő vagy másodlagos SSID-t a biztonság konfigurálásához.
- **WPA Algorithms (WPA algoritmus):**TKIP [Temporal Key Integrity Protocol] vagy AES [Advanced Encryption Standard]. A TKIP az alapértelmezett mód.
- **Pass Phrase (kulcskifejezés):**Itt 8-63 ASCII karakterrel adható meg a titkosító kifejezés.
- **Key Renewal Interval (a kulcs megújítási időköze):**Itt állítható be a kulcs megújítási időköze.

6.2.4 WPA- Enterprise

Ez a biztonsági mód akkor használatos, ha RADIUS kiszolgáló kapcsolódik az eszközhöz. A legördülő listán a „WPA-Enterprise" kijelölése esetén a következő ablak jelenik meg:

- **Select SSID (SSID választás)**：A legördülő menün kiválaszthatja a fő vagy másodlagos SSID-t a biztonság konfigurálásához.
- **WPA Algorithms (WPA algoritmusok)**：TKIP [Temporal Key Integrity Protocol] vagy AES [Advanced Encryption Standard]. A TKIP az alapértelmezett mód.
- **Key Renewal Interval (a kulcs megújítási időköze)**: Itt állítható be a kulcs megújítási időköze.
- **Radius Server (Radius kiszolgáló):**Itt kell megadni a Radius kiszolgáló IP-címét.
- **Radius Server port (a Radius kiszolgáló portja):**Itt kell megadni a Radius kiszolgáló hitelesítő portját. Az alapértelmezett portszám 1812.
- **Shared Secret (közös titok):**8–63 ASCII karakterrel adja meg a közös kulcsot a hitelesítő szervernek.
- **Session Timeout (a munkamenet időkorlátja):**Az AP hozzáférési pont és a hitelesítő kiszolgáló közötti hitelesítési időszak hossza.

6.2.5 WPA2-Enterprise

A titkosítási mód Radius hitelesítő kiszolgálóra és WPA2 titkosítási módra épül. A WPA2 akkor használatos, ha RADIUS kiszolgáló kapcsolódik az eszközhöz. A legördülő listán a „WPA2-Enterprise" kijelölése esetén a következő ablak jelenik meg:

- **Select SSID (SSID választás):**A legördülő menün kiválaszthatja a fő vagy másodlagos SSID-t a biztonság konfigurálásához.
- **WPA Algorithms (WPA algoritmus):**TKIP [Temporal Key Integrity Protocol] vagy AES [Advanced Encryption Standard]. A TKIP az alapértelmezett mód.
- **Key Renewal Interval (a kulcs megújítási időköze):**Itt állítható be a kulcs megújítási időköze.
- **Radius Server (Radius kiszolgáló):**Itt kell megadni a Radius kiszolgáló IP-címét.
- **Radius Server port (a Radius kiszolgáló portja):**Itt kell megadni a Radius kiszolgáló hitelesítő portját. Az alapértelmezett portszám 1812.

- **Shared Secret (közös titok):**8–63 ASCII karakterrel adja meg a közös kulcsot a hitelesítő szervernek.
- **Session Timeout (a munkamenet időkorlátja):**Az AP hozzáférési pont és a hitelesítő kiszolgáló közötti hitelesítési időszak hossza. Az alapértelmezett időszak 3600 s.

6.2.6 802.1X

Ez a biztonsági mód akkor használatos, ha RADIUS kiszolgáló kapcsolódik az eszközhöz. A port-alapú hitelesítési protokollként működő 802.1x a felhasználók rendelkezésére álló hitelesítési típus és stratégia. A port lehet fizikai vagy logikai (például VLAN). Vezeték nélküli LAN használóknál a port ugyanaz, mint a csatorna. A 802.1x hitelesítés végső célja a port használhatóságának ellenőrzése. A sikeresen hitelesített port megnyitható üzenetek továbbítására. Ha a port hitelesítése sikertelen, akkor „disabled" (letiltott) állapotban tartható a port; ilyenkor csak a 802.1x hitelesítési protokoll üzenetei mehetnek át rajta. A legördülő listán a „802.1x" kijelölése esetén a következő ablak jelenik meg:

- **Select SSID (SSID választás):**A legördülő menün kiválaszthatja a fő vagy másodlagos SSID-t a biztonság konfigurálásához.
- **WEP**: A WEP algoritmus az „Enable" lehetőséggel engedélyezhető, a „Disable" lehetőséggel letiltható.
- **Radius Server**: Itt kell megadni a Radius kiszolgáló IP-címét.
- **Radius Server Port (a Radius kiszolgáló portja):**Itt kell megadni a Radius kiszolgáló hitelesítő portját. Az alapértelmezett portszám 1812.
- **Shared Secret (közös titok):**8–63 ASCII karakterrel adja meg a közös kulcsot a hitelesítő szervernek.
- **Session Timeout (a munkamenet időkorlátja)**: Az AP hozzáférési pont és a hitelesítő kiszolgáló közötti hitelesítési időszak hossza. Az alapértelmezett időszak 3600 s.

6.4 WPS beállítás

A WPS (Wi-Fi Protected Setting) segítségével könnyen és gyorsan titkosítható a vezeték nélküli hálózati ügyfelek és az eszköz közötti kapcsolat. A felhasználóknak csak a PIN-kódot kell megadniuk vagy kezelőpanelen levő WPS gombot kell megnyomniuk; nem szükséges kézzel megadniuk a titkosítási módszert és a titkos kulcsokat. A „Wireless settings" (Vezeték nélküli beállítások) menü „WPS settings" (WPS beállítások) pontjára kattintáskor a következő képernyő jelenik meg.

- **WPS settings (WPS beállítások)**: Itt lehet be- és kikapcsolni a WPS funkciót. Alapértelmezésben ki van kapcsolva („disable").
- **WPS mode (WPS mód):**Kétféle lehetőség van: PBC (Push-Button Configuration, azaz nyomógombos konfigurálás) és PIN-kód.
- **PBC**: Válassza ki a PBC lehetőséget vagy nyomja meg kb. 1 másodpercre az eszköz előlapján levő WPS gombot (Tartsa nyomva a gombot kb. egy másodpercig. Ekkor a WPS jelző 2 percig villogni fog, ezzel jelezve a WPS bekapcsolt állapotát. Miközben villog, engedélyezhet más eszközt a WPS/PBC egyeztetés végrehajtására. Két perc elteltével a WPS jelző kikapcsol, ami a WPS kapcsolat lezárultát jelzi. További ügyfelek hozzáadásához ismételje meg a fenti lépéseket. Pillanatnyilag legfeljebb 32 ügyfél elérését támogatja a WPS.)
- PIN: E lehetőség választásakor be kell írni a mezőbe a vezeték nélküli ügyfél PIN-kódját, és ugyanezt a kódot kell megadni a WPS ügyfélben.

6.5 WDS beállítások

A WDS (Wireless Distribution System) segítségével kiterjeszthető a vezeték nélküli rendszer által lefedett terület. Ez az útválasztó a következő három módot kínálja: Lazy (lusta), Bridge (híd) és Repeater (ismétlő).

Lazy (lusta): Ebben a módban a csatlakoztatott eszköz Bridge (híd) vagy Repeater (ismétlő) módban lehet. A kapcsolat létrehozásához meg kell adni az útválasztó BSSID kódját.

Bridge (híd): Ezzel a móddal két vagy több vezetékes hálózat vezeték nélkül kapcsolható össze. Ebben a módban hozzá kell adni a csatlakozó eszköz vezeték nélküli MAC címét az útválasztó AP MAC címtáblájához, vagy ki kell választani egy címet az eszközkeresési táblából.

Repeater Mode (ismétlő mód): Ebben a módban a partner MAC címét kézzel vagy eszközkeresővel (scanner) hozzá kell adni a saját AP MAC címtáblához a vezeték nélküli rádiókapcsolat kiterjesztéséhez.

7. fejezet: DHCP kiszolgáló

7.1 DHCP beállítások

A DHCP (Dynamic Host Control Protocol) IP-címet rendel a LAN/magánhálózat számítógépeihez. A DHCP kiszolgáló engedélyezésekor a DHCP kiszolgáló automatikusan hozzárendel egy szabad címet a kérést küldő számítógéphez a rendelkezésre álló IP-cím tartományból, „Obtain an IP Address Automatically" (IP-cím automatikus kérése) aktiválás feltételezésével. A hozzárendelés működéséhez meg kell adni az IP-cím tartomány első és utolsó címét.

- **DHCP kiszolgáló:** A DHCP kiszolgáló engedélyezéséhez jelölje be a négyzetet.
- **IP Address Start/End (első/utolsó IP-cím):** Adja meg a DHCP kiszolgálónak az IP-cím tartomány első és utolsó címét.
- **Lease Time (bérlési idő):** Az IP-cím bérlési ideje.

8. fejezet: Firmware frissítés

8.1 Az útválasztóba épített firmware frissítéséhez töltse le a frissítőcsomagot a www.nedis.nl címről, keresse meg a letöltött csomagot, és kattintson az „Upgrade" (Frissítés) gombra.

- **Browse (Tallózás)**: Kattintson erre a gombra a frissítőcsomag kiválasztásához.
- **Upgrade (Frissítés)**: Kattintson erre a gombra a frissítés elindításához. A frissítés befejeztével az útválasztó automatikusan újraindul.

8.2 Az útválasztó újraindítása

Az útválasztó újraindításával érvényesíteni lehet a konfigurált beállításokat vagy újra be lehet állítani az útválasztót, ha nem sikerült a beállítás.

8.3 Jelszómódosítás

A következők szerint lehet új felhasználói nevet és jelszót megadni, az útválasztó és a hálózat biztonságosabbá tételéhez.

- **User Name (Felhasználónév)**: Itt lehet megadni új felhasználói nevet az eszközhöz.
- **Old Password (Régi jelszó):** Ide kell beírni a régi jelszót.
- **New Password (Új jelszó):** Ide kell beírni az új jelszót.
- **Re-enter to Confirm (Jelszó megerősítése):** Ide kell még egyszer beírni az új jelszót.

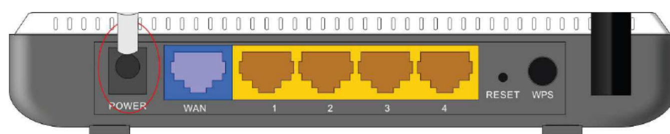
8.4 Kijelentkezés

A konfigurálás befejeztével a webes kezelőfelület logout (kijelentkező) oldalán a „Yes" (Igen) gombra kattintással lehet kijelentkezni a kezelőfelületről.

Útválasztó üzembe helyezése és beállítása kábeles vagy ADSL modemhez

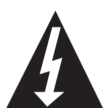
Figyelmeztetés!
Az alábbi lépések közül egyet se hagyjon ki!

1. Kapcsolja ki a modemet (húzza ki tápegységét).
2. Kapcsolja ki a számítógépet.
3. **LAN kábellel** kösse össze a modem **LAN kimenetét** az útválasztó **kék csatlakozójával**.
4. **LAN kábellel** kösse össze az egyik **sárga csatlakozót** a számítógép csatlakozójával.



5. Most kapcsolja be a modemet és várja meg, hogy felcsatlakozzon (várja ki türelmesen).
6. Kapcsolja be az útválasztót és várjon legalább 30 másodpercet.
7. Kapcsolja be a számítógépet és várja meg, hogy teljesen betöltődjön.
8. Nyissa meg a böngészőt és írja a címsorába a http://192.168.0.1. címet.
9. Írja be a felhasználói nevet és a jelszót (alapértelmezésben mindkettő **admin**).
10. Keresse meg a **Setup Wizard** beállító varázslót és kattintson az **Auto Detect** pontra.
11. Kattintson a **Next** gombra, majd az **Apply** gombra.
12. Nyissa meg a **WLAN settings** menüt és ellenőrizze, hogy be van-e jelölve az **Enable Wireless** négyzet.
13. Itt megadhatja hálózata nevét (SSID) és a csatornát.
14. Nyissa meg a **Security Settings** almenüt és válassza ki a biztonsági védelem típusát. A **Mixed WPA/WPA2 – Personal** lehetőség választását ajánljuk.
15. A **WPA Algorithms** alatt a **TKIP&AES** lehetőséget válassza ki.
16. A **Pass Phrase** mezőben módosítsa a jelszót. Javasoljuk, hogy erős jelszót adjon meg, amelyben betűk, számok és speciális jelek egyaránt vannak.
17. Az adatok elmentéséhez kattintson az **Apply** gombra.
18. Lépjen ki a böngészőből; befejezte vezeték nélküli hálózata és biztonsági beállításai megadását. Ha számítógépe vezeték nélküli hálózati csatlakozásra is fel van készítve, az útválasztó és a számítógép közötti kábelt lekötheti.

Biztonsági óvintézkedések:



VIGYÁZAT!

ÁRAMÜTÉS VESZÉLYE!
NE NYISSA FEL!



Az áramütés veszélyének csökkentése érdekében ezt a terméket KIZÁRÓLAG a márkaszerviz képviselője nyithatja fel. Hiba esetén húzza ki a termék csatlakozóját a konnektorból, és kösse le más berendezésekről. Vigyázzon, hogy ne érje a terméket víz vagy nedvesség.

Karbantartás:

Csak száraz ronggyal tisztítsa. Tisztító- és súrolószerek használatát mellőzze.

Jótállás:

Nem vállalunk jótállást és felelősséget a terméken végzett változtatás vagy módosítás vagy a termék helytelen használata miatt bekövetkező károkért.

Általános tudnivalók:

- A kivitel és a műszaki jellemzők előzetes értesítés nélkül is módosulhatnak.
- Minden logó, terméknév és márkanév a tulajdonosának márkaneve vagy bejegyzett márkaneve, azokat ennek tiszteletben tartásával említjük.
- Jelen útmutató nagy gonddal készült. Ennek ellenére abból jogok nem származnak. A König Electronic nem felelős az útmutató hibáiért, vagy azok következményeiért.
- Őrizze meg ezt az útmutatót és a csomagolást.

Figyelem:



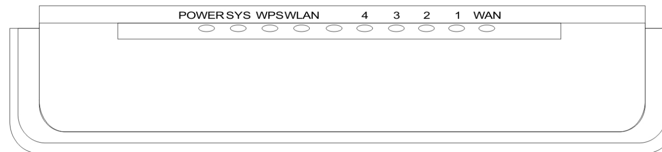
Ezt a terméket ezzel a jelöléssel láttuk el. Azt jelenti, hogy az elhasznált elektromos és elektronikus termékeket tilos az általános háztartási hulladékhoz keverni. Begyűjtésüket külön begyűjtő létesítmények végzik.

SUOMI

Luku 1: Johdanto

1.1 LED.merkkivalo ja porttien kuvaus

Etupaneeli ja LED-merkkivalonäyttö



LED -merkkivalojen kuvaus etupaneelissa: (vasemmalta oikealle)

- **POWER**

  Vihreän valon jäädessä palamaan se osoittaa, että virta on kytketty oikein.

- **SYS**

  Kun vihreä valo vilkkuu, se osoittaa, että järjestelmä on oikein käynnissä.

- **WPS**

  Kun tämä välkkyy, se osoittaa, että laite neuvottelee asiaskoneen kanssa WPS-tilassa.

- **WLAN**

  Langattoman signaalin LED-merkkivalo. Kun vihreä valo vilkkuu, se osoittaa, että langaton toiminto on käytössä.

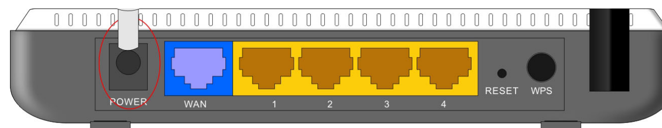
- **LAN (4, 3, 2, 1)**

  Langallisen paikallisen verkon LED-merkkivalo. Jos merkkivalo palaa, se osoittaa, että se on liitetty Ethernet-laitteeseen; vilkkuminen osoittaa, että laite lähettää ja/tai vastaanottaa tietoja.

- **WAN**

  Alueverkon merkkivalo. Jos valo jää palamaan, se osoittaa reitittimen W.

Takapaneelin näyttö:



Takapaneeli: (vasemmalta oikealle)

- **POWER**

Liitin on virtasovittimen liittämistä varten. Käytä mukana tulevaa 9V:n DC virtasovitinta.

- **WAN**

100Mb/s Ethernet-portti, joka voidaan yhdistää MODEEMIN, kytkimen, reitittimen ja muiden Ethernet-laitteiden kanssa Internet-yhteyden luomiseksi DSL- tai kaapelimodeemin ja ISP:iin.

- **LAN (1, 2, 3, 4)**

4 10/100Mb/s Ethernet-portit voidaan liittää Ethernet-kytkimeen, reitittimeen ja NIC-korttiin.

- **RESET**

Järjestelmän resetointipainike. Paina painiketta 7 sekunnin ajan, tähän laitteeseen määritellyt asetukset poistetaan ja oletusasetukset palautetaan.

- **WPS**

Paina tätä 1 sekunnin ajan. WPS-ominaisuus otetaan käyttöön ja WPS-osoitin välkkyy.

Luku 2: Laitteiston asennus

2.1 Kuinka reititin asennetaan

Käytä mukana tulevaa virtasovitinta reitittimen virtalähteenä. TÄRKEÄÄ: Muun virtasovittimen käyttö voi aiheuttaa vaurioita ja tämän laitteen takuun peruuntumisen. Liitä reitittimen LAN-portti tietokoneesi verkkosovittimeen kaapelilla. Yhdistä palveluntarjoajan tarjoama laajakaistalinjasi WAN-porttiin. Aseta mukana tuleva CD-ROM CD-ROM-asemaan, kaksoisnapsauta ”Setup” -kuvaketta ja noudata ohjeita asennuksen loppuun saattamiseksi. Tai voit antaa reitittimen verkkosivun sen määrittämiseksi. (Lisätietoja luvusta 3.)

Luku 3: Kirjautuminen reitittimelle

3.1 Kuinka verkonmäärittelyt tehdään

1. Napsauta hiiren oikealla tietokoneen työpöydällä ”My Network Places” (Verkkoympäristö) ja Valitse ”Properties” (Ominaisuudet).
2. Napauta hiiren oikealla ”Local Area Network Connection” (Lähiverkkoyhteys) ja valitse ”Properties” (Ominaisuudet).
3. Valitse ”Internet Protocol (TCP/IP)” ja napsauta ”Properties” (Ominaisuudet).
4. - Valitse ”Obtain an IP address automatically” (Hae IP-osoite automaattisesti) ja ”Obtain DNS server address automatically” (Hae DNS-palvelimen osoite automaattisesti). Napsauta ”OK” tallentaaksesi konfiguraation.
   - Tai valitse ”Use following IP address” (Käytä seuraavaa IP-osoitetta) ja anna IP-osoite, aliverkon peite ja oletusyhdyskäytävä seuraavasti: IP-osoite: 192.168.0.XXX: (XXX on numero välillä 2~254) Aliverkon peite: 255.255.255.0
   Gateway: 192.168.0.1 Palveluntarjoajan antama DNS-palvelimen osoite täytyy ehdottomasti syöttää. Muutoin voit käyttää reitittimen oletusyhdyskäytävää DNS:n välityspalvelinta. Napsauta ”OK” tallentaaksesi konfiguraation.

3.2 Kirjaudu reitittimelle

1. Siirtyäksesi reitittimen verkkopohjaiseen liitäntään, avaa verkkoselain, kuten Internet Explorer tai Firefox ja anna reitittimen oletus IP-osoite, http://192.168.0.1. Paina ”Enter”.
2. Syötä ”admin” sekä käyttäjänimen että salasanan kohdalle. Napsauta ”OK”.

oletusasetus	
IP-osoite	192.168.0.1
Salasana	admin
SSID	KONIG
Turvallisuustila	Pois käytöstä
Langaton tila	b/g/n sekoitettu tila
Kanava	Autoselect
Aikavyöhyke	
WPS-asetukset	Ota käyttöön
UPNP Laitteen nimi	11N Langaton laajakaistareititin
UPNP:n valmistaja	KONIGELECTRONIC
UPNP Mallin nro	CMP-WNROUT41
UPNP Mallin nro	V 1.0
UPNP raportoima verkon nopeus	300Mb/s
UPNP Laitteen osoite	http://192.168.0.1
UPNP	Ota pois käytöstä

Luku 4: Pika-asetusopas

4.1 Asennusavustaja

Tämä on ”Tervetuloa asennusavustajaan”, jotta reitittimesi konfigurointi olisi nopeaa. Napauta ”Next” (Seuraava).

Valitse tällä ruudulla yksi Internet-yhteyden tila, jota käytät. Jos et ole varma, paina ”Detect” (Etsi) -painiketta, tai ota yhteyttä palveluntarjoajaasi, ja napsauta ”Next” (Seuraava).

ADSL Virtual Dial-up (Via PPPoE)

Anna palveluntarjoajan antama tili ja salasana, ja napsauta ”Next” (Seuraava)..

Dynaaminen IP (DHCP:n kautta)

Jos yhteystilasi on dynaaminen IP, se tarkoittaa, että IP-osoitteesi muuttuu joka kerta, kun muodostat yhteyden. Tietoja ei tarvitse antaa samalla tavoin kuin muissa tiloissa. Napsauta ”Next” (Seuraava) ja ”Save” (Tallenna) lopettaaksesi asetukset.

Staattinen IP

Tässä ruudussa anna palveluntarjoajasi verkko-osoitetiedot kohtiin IP-osoite, aliverkon peite, yhdyskäytävä ja ensisijainen DNS palvelin, ja napsauta ”Next” (Seuraava).

L2TP

Ota yhteyttä palvelun tarjoajaasi saadaksesi tarvittavat tiedot.

Luku 5: Lisäasetukset

5.1 LAN-asetukset

LAN-asetukset ovat LAN-porttien perus-TCP/IP-parametrejä varten.

- **IP Address**: Reitittimen LAN IP-osoitteet (ei tietokoneen IP-osoite). 192.168.0.1 on oletusasetus.
- **Subnet Mask**: Se näyttää reitittimen aliverkon peitteen verkon koon mittaamiseksi. 255.255.255.0 on oletusasetus.

TÄRKEÄÄ:

Kun muokkaat IP-osoitetta, se täytyy muistaa verkkopohjaiselle laitteen kirjautumiselle seuraavalla kerralla.

5.2 WAN-asetukset

Kun olet valunnut palveluntarjoajan yhteystyypin asennusavustajassa, ja haluat muokata niihin liittyviä asetuksia, voit muokata ja määritellä asetukset yksityiskohtaisesti tässä.

Staattinen IP

Jos yhteystavaksi on valittu staattinen IP, voit muokata seuraavia osoitetietoja.

- **IP Address**: Anna ISP:si antama WAN IP-osoite tähän.
- **Subnet Mask**: Syötä WAN:n aliverkon peite tähän.
- **Gateway**: Syötä WAN:n yhdyskäytävän osoite tähän.
- **Primary DNS Server**: Anna ISP:n antaman ensisijainen DNS-palvelin tähän.
- **Secondary DNS Server**: Anna toissijainen DNS.

Luku 6: Langattomat asetukset

6.1 Perusasetukset

- **Enable Wireless**: Valitse tämä ottaaksesi reitittimen langattomat ominaisuudet käyttöön; poista valinta ottaaksesi ominaisuuden pois käytöstä.
- **Network Mode**: Valitse yksi tila seuraavista. Oletus on 11b/g/n -tila.
- **Main SSID**: SSID (Service Set Identifier) on langattoman verkon ainutkertainen nimi. Tällä laitteella on kaksi SSID:ä ja pää-SSID on tarpeen.
- **Minor SSID**: Tämä on valinnainen.

- **Broadcast (SSID)**: Valitse ”Enable”, jotta laitteen SSID on näkyvissä langattomille asiakkaille. Oletus on käytössä (enabled).
- **MBSSID AP Isolation**: Pääsynhallintaominaisuus, joka perustuu langattomaan MAC-osoitteeseen. Kun tämä ominaisuus on käytössä, samaan SSID:iin yhdistäneet langattomat asiakaskoneet eivät voi kommunikoida toistensa kanssa.
- **AP Isolation**: Pääsynhallintaominaisuus, joka perustuu SSID:iin. Kun tämä ominaisuus on käytössä, kukin langattomasti asiakaskoneista on omassa virtuaalisessa verkossaan, eikä voi kommunikoida muiden kanssa. Kun tämä ominaisuus on käytössä, langattomat laitteet, jotka ovat yhdistäneet Main SSID:iin ja Minor SSID:iin eivät voi kommunikoida keskenään, joka voi vaikuttaa merkittävästi langattomaan verkkoon.
- **Channel**: Määritä langattoman verkon voimassa oleva kanava (1 - 13\Auto).
- **Extension Channel**: Lisätäksesi langattoman verkon tiedon suorituskykyä, laajennuskanavan aluetta käytetään 11n-tilassa.
- **Channel Bandwidth**: Valitse kanavan kaistanleveys parantaaksesi langatonta suorituskykyä. Kun verkolla on 11b/g ja 11n asiakaskoneita, voita valita 40M:n; kun se on 11n verkossa, valitse 20/40M parantaaksesi sen suorituskykyä.

6.2 Langattomat tietoturva-asetukset

Tätä käytetään määrittämään tukiaseman verkon tietoturva-asetus. Tässä esitellään kuusi (yhteensä kymmenen) yleistä salausmetodia, mukaan lukien Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, jne.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), perussalausmenetelmä, joka yleensä salaa langattoman datan, joka käyttää digitaalisten avainten sarjaa (pituudeltaan 64-bittistä tai 128-bittistä). Käyttämällä samoja avaimia kussakin langattoman verkon laitteessasi, voit estää valtuuttamattomien laitteiden pääsen lähetystesi seuraamisen tai langattomien resurssiesi käyttämisen. Valitse ”Mixed WEP” siirtyäksesi seuraavaan ikkunaan:

- **Select SSID**: Valitse SSID (main SSID tai minor SSID) määrittääksesi tietoturva-asetukset pudotusvalikosta.
- **Security Mode**: Valitse pudotusvalikosta vastaavat tietoturvan salaustilat.
- **WEP Key1~4**: Aseta WEP-avain ASCII:lla ja heksamuodossa. Voit antaa ASCII-koodin (5 tai 13 ASCII merkkiä. Merkkejä kuten ”/” ei sallita) tai 10/26 heksamerkkejä.
- **Default Key**: Valitse yksi avain neljästä määritellystä avaimesta nykyiseksi käytettäväksi.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), Wi-Fi standardi, on uudempi langaton salaustapa, joka on suunniteltu parantamaan WEP:n tietoturva-ominaisuuksia. Se ottaa käyttöön tehokkaammat salaustyypit (kuten TKIP [Temporal Key Integrity Protocol] tai AES [Advanced Encryption Standard]) ja voi muuttaa avaimia dynaamisesti jokaisessa valtuutetussa langattomassa laitteessa.

- **Select SSID**: Valitse SSID (main SSID tai minor SSID) määrittääksesi tietoturva-asetukset pudotusvalikosta.
- **WPA Algorithms**: Antaa TKIP:n [Temporal Key Integrity Protocol] tai AES:n [Advanced Encryption Standard]. Oletus on TKIP-tila.
- **Pass Phrase**: Anna salatut merkti 8-63 ASCII-merkillä.
- **Key Renewal Interval**: Aseta avaimen uudistumisaika.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) tarjoaa paremman tietoturvan kuin WEP (Wireless Equivalent Privacy) ja WPA (Wi-Fi Protected Access).

- **Select SSID**: Valitse SSID (main SSID tai minor SSID) määrittääksesi tietoturva-asetukset pudotusvalikosta.
- **WPA Algorithms**: Antaa TKIP:n [Temporal Key Integrity Protocol] tai AES:n [Advanced Encryption Standard]. Oletus on TKIP-tila.
- **Pass Phrase**: Anna salatut merkit 8-63 ASCII-merkillä.
- **Key Renewal Interval**: Aseta avaimen uudistumisaika.

6.2.4 WPA- Enterprise

Tätä turvatilaa käytetään, kun RADIUS-palvelin on liitetty laitteeseen. Valitse ”WPA-Enterprise” pudotusvalikosta siirtyäksesi seuraavaan ikkunaan:

- **Valitse SSID**：Valitse SSID (main SSID tai minor SSID) määrittääksesi tietoturva-asetukset pudotusvalikosta.
- **WPA Algorithms**：Antaa TKIP:n [Temporal Key Integrity Protocol] tai AES:n [Advanced Encryption Standard]. Oletus on TKIP-tila.
- **Key Renewal Interval**: Aseta avaimen uudistumisaika.
- **Radius Server**: Anna Radius-palvelimen IP-osoite.
- **Radius Server port**: Anna Radius-palvelimen autentikointiportti. Oletus on 1812.
- **Shared Secret**: Anna jaettu avain autentikointipalvelimelle 8~63 ASCII merkillä.
- **Session Timeout**: Autentikointiväli AP:n ja autentikointipalvelimen välillä.

6.2.5 WPA2-Enterprise

Tämä tietoturvatila perustuu Radiuksen autentikointipalvelimeen ja WPA2-salaustapaan. WPA2:a käytetään, kun RADIUS-palvelun on liitetty laitteeseen. Valitse pudotusvalikosta ”WPA2-Enterprise” siirtyäksesi seuraavaan ikkunaan:

- **Select SSID**: Valitse SSID (main SSID tai minor SSID) määrittääksesi tietoturva-asetukset pudotusvalikosta.
- **WPA Algorithms**: Antaa TKIP:n [Temporal Key Integrity Protocol] tai AES:n [Advanced Encryption Standard]. Oletus on TKIP-tila.
- **Key Renewal Interval**: Aseta avaimen uudistumisaika.
- **Radius Server**: Anna Radius-palvelimen IP-osoite.
- **Radius Server port**: Anna Radius-palvelimen autentikointiportti. Oletus on 1812.
- **Shared Secret**: Anna jaettu avain autentikointipalvelimelle 8~63 ASCII merkillä.
- **Session Timeout**: Autentikointiväli tukiaseman ja autentikointipalvelimen välillä. Oletus on 3600 s.

6.2.6 802.1X

Tätä tietoturvatilaa käytetään, kun RADIUS-palvelin on liitetty laitteeseen. 802.1x on eräänlainen porttipohjainen autentikointiprotokolla, autentikointityyppi ja strategia käyttäjille. Portti voi olla joko fyysinen portti tai looginen portti (kuten VLAN). Langattoman lähiverkon käyttäjille portti on vain kanava. 802.11x autentikoinnin lopullinen tarkoitus on tarkastaa, voidaanko porttia käyttää. Jos portti on autentikoitu onnistuneesti, voit avata tämän portin, joka päästää kaikki viestit läpi. Jos porttia ei ole autentikoitu onnistuneesti, voit pitää tämän portin pois käytöstä (”disabled”), mikä sallii vain 802.1x autentikointiprotokollan viestin pääsyn läpi. Valitse ”802.1x” pudotusvalikosta siirtyäksesi seuraavaan ikkunaan:

- **Select SSID**: Valitse SSID (main SSID tai minor SSID) määrittääksesi tietoturva-asetukset pudotusvalikosta.
- **WEP**: Napsauta ”Enable/Disable” (Ota käyttöön/pois käytöstä) ottaaksesi WEP-algoritmin käyttöön tai pois käytöstä.
- **Radius Server**: Anna Radius-palvelimen IP-osoite.
- **Radius Server Port**: Anna Radius-palvelimen autentikointiportti. Oletus on 1812.

- **Shared Secret**: Anna jaettu avain autentikointipalvelimelle 8~63 ASCII merkillä.
- **Session Timeout**: Autentikointiväli tukiaseman ja autentikointipalvelimen välillä. Oletus on 3600 s.

6.4 WPS-asetukset

WPS-asetusta (Wi-Fi Protected Setting) voidaan käyttää helposti ja nopeasti yhteyden muodostamiseen langattomien verkkoasiakkaiden ja laitteen välillä. Käyttäjät syöttävät vain PIN-koodin tai painavat paneelin WPS-painiketta määritelläkseen sen manuaalisest valitsemalla salaustavan ja salaisen avaimen.

Napsauta ”Wireless settings” -valikossa ”WPS settings” siirtyäksesi seuraavaan ruutuun.

- **WPS settings**: Ota WPS-toiminto käyttöön tai pois käytöstä. Oletus on ”pois käytöstä”. (disable)
- **WPS mode**: Kaksi eri tapaa: PBC (Push-Button Configuration) ja PIN-koodi.
- **PBC**: Valitse PBC tai Paina WPS-painiketta laitteen etupaneelissa noin sekunnin ajan (Paina painiketta noin sekunnin ajan ja WPS-merkkivalo välkkyy 2 minuuttia, joka tarkoittaa, että WPS on käytössä. Valon vilkkuessa voit ottaa käyttöön toisen laitteen ottaaksesi käyttöön niiden välisen WPS/PBC-neuvottelun. Kahden minuutin jälkeen WPS-merkkivalo sammuu, joka tarkoittaa, että WPS-yhteys on valmis. Jos lisää asiakkaita lisätään, toista yllä olevat vaiheet. Nykyisellään WPS tukee 32 asiakaskoneen pääsyä.)
- PIN: Jos tämä valinta on käytössä, anna langattoman asiakaskoneen Pin-koodi kentään ja pidä sama koodi WPS-asiakaskoneella.

6.5 WDS-asetukset

WDS (Wireless Distribution System) -järjestelmää käytetään laajentamaan peittoaluetta. Tässä reitittimessä on kolme eri tilaa: Lazy, Bridge ja Repeater.

Lazy: Tässä tilassa yhdistetty laite voi olla sillatussa tilassa tai toistintilassa, ja anna reitittimen BSSID muodostaaksesi yhteyden.

Bridge: Voit yhdistää langattomasti kahteen tai useampaan langattomaan verkkoon tämän tilan kautta. Tässä tilassa täytyy lisätä yhdistettävän laitteen langaton MAC-osoite reitittimen tukiaseman MAC-osoitetaulukkoon tai valitse yksi skannaustaulukosta.

Repeater Mode: Lisää tässä tilassa vastakkainen MAC-osoite kunkin omaan tukiaseman MAC-osoitetaulukkoon manuaalisesti tai skannerin kautta suurentaaksesi tai laajentaaksesi langatonta kantamaa.

Luku 7: DHCP-palvelin

7.1 DHCP-asetukset

DHCP (Dynamic Host Control Protocol) antaa IP-osoitteet LAN/yksityisen verkon tietokoneille. Kun otat DHCP-palvelimen käyttöön, DHCP-palvelin antaa automaattisesti käyttämättömän IP-osoitteen IP-osoitejoukosta pyytävälle tietokoneelle aktivoitaessa ”Obtain an IP Address Automatically” (Nouda IP-osoite automaattisesti). Joten IP-osoitteen alun ja lopun määrittelyä tarvitaan.

- **DHCP Server**: Aktivoi valintaruutu ottaaksesi käyttöön DHCP-palvelimen.
- **IP Address Start/End**: Anna IP-osoitteiden alue DHCP:n palvelimen jakoa varten.
- **Lease Time**: IP-osoitteen vuokra-aika.

Luku 8: Päivitä laiteohjelmisto

8.1 Reititn tarjoaa laiteohjelmiston päivityksen napsauttamalla ”Upgrade” (Päivitä) laiteohjelmiston päivityspaketin haun jälkeen, jonka voit ladata osoitteesta www.nedis.nl

- **Browse**: Napsauta tätä painiketta valitaksesi päivitystiedoston.
- **Upgrade**: Napsauta tätä painiketta aloittaaksesi päivitysprosessin. Kun päivitys on tehty, reititin käynnistyy uudelleen automaattisesti.

8.2 Reitittimen uudelleenkäynnistys

Reitittimen uudelleenkäynnistys ottaa määritetyt asetukset voimaan tai asettaa reitittimen uudelleen, jos asetukset ovat epäonnistuneet.

8.3 Salasanan muuttaminen

Tämä osio on uuden käyttäjänimen ja salasanan asettamiseen, jotta voit salata reitittimen ja verkon.

- **User Name**: Anna laitteelle uusi käyttäjänimi.
- **Old Password**: Anna vanha salasana.
- **New Password**: Anna uusi salasana.
- **Re-enter to Confirm**: Syötä uudelleen vahvistaaksesi uuden salasanan.

8.4 Uloskirjautuminen

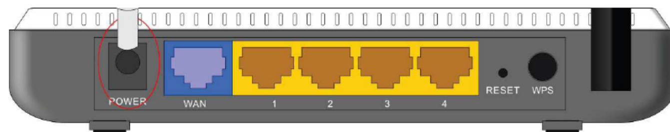
Kun olet lopettanut asetusten tekemisen kokonaan, napsauta ”Yes” (Kyllä) uloskirjautumissivulla kirjautuaksesi ulos verkonhallintasivulta.

Kuinka reititin asennetaan ja sen asetukset tehdään kaapeli- tai ADSL-modeemiin

Huomio!

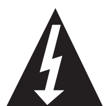
Noudata näitä ohjeita ohittamatta mitään vaihetta

1. Sammuta modeemi (irrota verkkovirrasta).
2. Sammuta tietokone.
3. Liitä modeemin **LAN-lähtö LAN-kaapelilla** reittimen **siniseen porttiin.**
4. Liitä yksi **keltaisista porteista LAN-kaapelilla** tietokoneeseen.



5. Kytke nyt modeemi päälle ja odota, kunnes se on on muodostanut yhteyden kokonaan (tämä voi viedä jonkin aikaa).
6. Kytke reititin päälle ja odota vähintään 30 sekuntia.
7. Käynnistä tietokone ja odota, kunnes se on täysin käynnistynyt.
8. Avaa selaimesi ja syötä osoiteriville osoite http://192.168.0.1.
9. Syötä käyttäjänimi ja salasana (molemmat oletuksena: **admin**).
10. Siirry kohtaan **Setup Wizzard** (Asennusavustaja) ja napauta **Auto Detec** (Etsi automaattisesti).
11. Napauta nyt **Next ja** seuraavassa ruudussa napauta **Apply**.
12. Siirry valikkoon **WLAN settings** (WLAN-asetukset) ja varmista, että **Enable Wireless** (Ota langaton käyttöön**)** on valittuna.
13. Tässä voit määritellä verkkosi nimen (SSID) ja kanavan.
14. Mene alavalikkoon **Security Settings** (Turva-asetukset) ja valitse tietoturvan tyyppi. Suosittelemme aina valitsemaan kohdan **Mixed WPA/WPA2 – Personal**.
15. Valitse **WPA Algorithms** -kohdassa **TKIP&AES**.
16. Muuta salasanaa kohdassa **Pass Phrase** (Salasana) Suosittelemme valitsemaan vahvan salasanan, joka koostuu kirjaimista, numeroista ja mahdollisesti yhdestä tai useammasta erikoismerkistä.
17. Napauta **Apply** (Ota käyttöön) tallentaaksesi tiedot.
18. Poistu selainikkunasta; langaton verkkosi ja tietoturva-asetukset ovat valmiit. Vaihtoehtoisesti voit irrottaa reitittimen ja tietokoneen välisen kaapelin langattoman yhteyden muodostamiseksi (jos tietokoneessasi on langaton vastaanotin).

Turvallisuuteen liittyvät varoitukset:






Sähköiskun riskin pienentämiseksi, AINOASTAAN valtuutettu huoltohenkilö saa avata tämän laitteen huoltoa varten. Jos ongelmia ilmenee, irrota laite verkkovirrasta ja muista laitteista. Älä altista laitetta vedelle äläkä kosteudelle.

Huolto:

Puhdista ainoastaan kuivalla kankaalla. Älä käytä liuottimia tai hankausaineita.

Takuu:

Takuu ja vastuuvelvollisuus mitätöityvät, jos tuote vaurioituu siihen tehtyjen muutoksien tai sen väärinkäytön takia.

Yleistä:

- Muutoksia malliin ja teknisiin ominaisuuksiin voidaan tehdä ilmoituksetta.
- Kaikki logot, merkit ja tuotenimet ovat niiden vastaavien omistajien tuotemerkkejä tai rekisteröityjä tuotemerkkejä ja niitä on käsiteltävä sellaisina.
- Kaikki oikeudet pidätetään. König Electronic ei ole vastuussa mistään tämän käyttöohjeen sisältämistä virheistä tai niiden seurauksista.
- Säilytä käyttöohjeet ja pakkaus myöhempää käyttötarvetta varten.

Huomio:



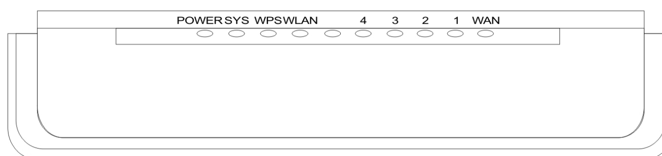
Tuote on varustettu tällä merkillä. Se merkitsee, ettei käytettyjä sähkö- tai elektronisia tuotteita saa hävittää kotitalousjätteen mukana. Kyseisille tuotteille on olemassa erillinen keräysjärjestelmä.

SVENSKA

Kapitel 1: Introduktion

1.1 LED-indikator och portbeskrivning

Främre panel och LED-indikatorsskärm



Beskrivning av LED-indikator på den främre panelen (från V till H)

- **STRÖM**

  När den gröna lampan lyser är strömmen påkopplad.
- **SYS**

  När den gröna lampan blinkar är systemet igång.
- **WPS**

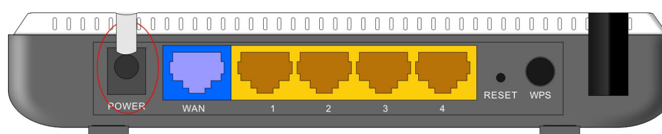
  När den blinkar söker anordningen efter klienter i WPS-läge.
- **WLAN**

  LED-indikator med trådlös signal. När den gröna lampan blinkar är den trådlösa funktionen aktiverad.
- **LAN (4, 3, 2, 1)**

  LED-indikator för fast lokalt nätverk. Om den lyser är den kopplad till ethernet-anordningen. Om den blinkar skickar och/eller tar anordningen emot data.
- **WAN**

  Indikator för Wide Area Network. Om den lyser visar den routerns W.

Bakre panelskärm



Bakre panel (Från V till H)

- **STRÖM**

Uttag för anslutning av strömadapter. Använd medföljande 9V likströms strömadapter.

- **WAN**

En 100 Mbps ethernetport som kan anslutas till modem, switch, router och andra ethernet-anordningar för Internetuppkoppling till DSL modem, kabelmodem och Internetleverantör.

- **LAN (1, 2, 3, 4)**

4 10/100 Mbps ethernet-portar kan anslutas med ethernet-switch, ethernet-router och nätverkskort.

- **ÅTERSTÄLLA**

Knapp för att återställa systemet. Om du trycker ned knappen i 7 sekunder kommer de konfigurerade inställningarna för anordningen att raderas och standardinställningarna att återställas.

- **WPS**

Om du trycker ned den i 1 sekund kommer WPS-funktionen att aktiveras och WPS-indikatorn att börja blinka.

Kapitel 2: Installera maskinvara

2.1 Installation av router

Använd medföljande strömadapter för att strömsätta routern. VIKTIGT! Om du använder en annan strömadapter kan det leda till skador och göra att produktgarantin annulleras. Anslut routerns LAN-port till

datorns nätverksadapter med en kabel. Anslut bredbandslinjen som du fått av din Internetleverantör till WAN-porten. Sätt i den medföljande CD-ROM-skivan i CD-ROM-spelaren, dubbelklicka på ikonen ”Setup” och följ instruktionerna för att avsluta installationen. Du kan också gå in på routerns webbsida för att göra konfigurationen. (För ytterligare information se kapitel 3.)

Kapitel 3: Logga in på routern

3.1 Inställning av nätverkskonfigurationer

1. Högerklicka på ”Mina nätverksplatser” på skrivbordet och välj ”Egenskaper”.
2. Högerklicka på ”Lokal nätverksanslutning” och välj ”Egenskaper”.
3. Välj ”Internetprotokoll (TCP/IP)” och klicka på ”Egenskaper”.
4. - Välj ”Erhåll en IP-adress automatiskt” och ”Erhåll adress till DNS-server automatiskt”. Klicka på ”OK” för att spara konfigurationerna.
   - Du kan också välja ”Använd följande IP-adress” och skriva in IP-adress, subnätmask och standardgateway enligt följande: IP-adress - 192.168.0.XXX (XXX är en siffra från 2 ... 254), subnätmask - 255.255.255.0,
   Gateway - 192.168.0.1, Du måste skriva in adressen till DNS-servern som du fått av din Internetleverantör. Annars kan du använda routerns standardgateway som proxyserver. Klicka på ”OK” för att spara konfigurationerna.

3.2 Logga in på routern

1. För att gå in på routerns webbaserade gränssnitt startar du en webbläsare som t.ex. Internet Explorer eller Firefox och går in på routerns standard IP-adress, http://192.168.0.1. Tryck på ”Enter”.
2. Logga in med ”administratör” för både användarnamn och lösenord. Klicka på ”OK”.

Standardinställning	
IP-adress	192.168.0.1
Lösenord	admin
SSID	KONIG
Säkerhetsläge	Inaktivera
Trådlöst läge	b/g/n blandat läge
Kanal	Automatiskt val
Tidszon	
WPS-inställningar	Aktivera
UPnP:s produktnamn	11N router för trådlöst bredband
UPnP:s tillverkare	KONIGELECTRONIC
UPnP:s modellnamn	CMP-WNROUT41
UPnP:s modellnummer	V 1.0
Rapporterad nätverkshastighet för UPnP	300 Mbps
UPnP:s produktadress	http://192.168.0.1
UPnP	Inaktivera

Kapitel 4: Snabbstartsguide

4.1 Igångsättningsguide

Detta är ”Välkommen till igångsättningsguiden” som hjälper dig att göra en snabb konfiguration av routern. Klicka på ”Nästa”.

Här väljer du den sorts Internetuppkoppling som du använder. Om du inte vet vilken det är kan du trycka på knappen ”Avkänning” eller kontakta din Internetleverantör. Klicka sedan på ”Nästa”.

ADSL, virtuell uppringning (via PPPoE)

Skriv in konto och lösenord som du fått av din Internetleverantör och klicka på ”Nästa”.

Dynamisk IP (via DHCP)

Om ditt anslutningsläge är dynamisk IP innebär det att din IP-adress ändras varje gång du ansluts. Du behöver inte föra in någon information som vid andra lägen. Klicka på ”Nästa” och ”Spara” för att avsluta inställningarna.

Statisk IP

Här för du in information om nätverksadressen från din Internetleverantör i fälten för IP-adress, subnätmask, gateway och primär DNS-server. Klicka sedan på ”Nästa”.

L2TP

Kontakta din Internetleverantör för att få den information som behövs.

Kapitel 5: Avancerade inställningar

5.1 LAN-inställningar

LAN-inställningar för LAN-portars grundparametrar TCP/IP.

- **IP-adress:** Routerns LAN:s IP-adresser (inte datorns IP-adress). 192.168.0.1 är standardvärdet.
- **Subnätmask:** Routerns subnätmask, för mätning av nätverkets storlek, visas. 255.255.255.0 är standardvärdet.

VIKTIGT!

När du väl ändrat IP-adressen måste du komma ihåg den eftersom den ska användas vid nästa inloggning på det webbaserade verktyget.

5.2 WAN-inställningar

När du valt Internetleverantörens anslutningsläge i ”Igångsättningsguiden” men vill ändra tillhörande inställningar kan du ändra och konfigurera inställningarna i detalj här.

Statisk IP

Om du valt statisk IP som anslutningsläge kan följande adressinformation ändras.

- **IP-adress**: Skriv in den IP-adress för WAN som du fått av din Internetleverantör här.
- **Subnätmask:** För in subnätmask för WAN här.
- **Gateway:** För in gateway för WAN här.
- **Primär DNS-server:** För in den primära DNS-servern du fått av din Internetleverantör.
- **Sekundär DNS-server:** För in sekundär DNS.

Kapitel 6: Trådlös inställningar

6.1 Grundinställningar

- **Aktivera trådlös:** Kryssa i för att aktivera routerns trådlösa funktioner och ta bort krysset för att inaktivera dem.
- **Nätverksläge:** Välj ett av följande lägen. Standardläge är 11b/g/n.
- **Huvudsakligt SSID:** SSID (Service Set Identifier) är det trådlösa nätverkets unika namn. Denna anordning har två SSID och det första är nödvändigt.
- **Ett andra SSID:** Detta är valbart.
- **Sändning (SSID):** Välj ”Aktivera” för att aktivera anordningens SSID så att det visas för trådlösa klienter. Standardinställningen är aktiverad.

- **Isolering av MBSSID AP:** En funktion med åtkomstkontroll som baseras på en trådlös MAC-adress. När funktionen är aktiverad kan inte trådlösa klienter som är anslutna till samma SSID kommunicera med varandra.
- **Isolering av AP:** En funktion med åtkomstkontroll som baseras på SSID. När funktionen är aktiverad kommer alla dina trådlösa klienter att vara i ett eget virtuellt nätverk utan att kunna kommunicera med varandra. När denna funktion är aktiverad kan inte trådlösa klienter som är anslutna till huvudsakligt SSID eller ett andra SSID kommunicera med varandra, vilket gör att skyddet för det trådlösa nätverket stärks.
- **Kanal:** Ange det trådlösa nätverkets verksamma kanal (från 1 till 13\automatiskt).
- **Kanaltillägg:** För att öka det trådlösa nätverkets datakapacitet används spannet för kanaltillägget i 11n-läge.
- **Kanalbandbredd:** Välj den kanalbandbredd som förbättrar den trådlösa prestandan. Om nätverket har 11b/g eller 11n-klienter kan du välja 40 M. Om det är ett 11n-nätverk väljer du 20/40 M för att förbättra dess datakapacitet.

6.2 Trådlösa säkerhetsinställningar

Används för att konfigurera AP-nätverkets säkerhetsinställningar. De sex (tio totalt) vanliga datakrypteringstyperna presenteras här, inklusive mixat WEP, WPA-personlig, WPA-företag, WPA2-personlig, WPA2-företag etc.

6.2.1 Mixat WEP

Grunddatakrypteringstypen WEP (Wired Equivalent Privacy) krypterar vanligtvis trådlös data med hjälp av en serie digitala nycklar (64 bits eller 128 bits långa). Genom att använda samma nycklar för alla dina trådlösa nätverksanordningar kan du förhindra att obehöriga trådlösa anordningar övervakar dina sändningar eller använder dina trådlösa resurser. Välj mixat WEP för att komma till följande fönster.

- **Välj SSID:** Välj SSID (huvudsakliga SSID eller andra SSID) för att konfigurera säkerhetsinställningar från rullgardinsmenyn.
- **Säkerhetsläge:** Från rullgardinsmenyn väljer du motsvarande säkerhetskrypteringslägen.
- **WEP-nyckel 1 ... 4:** Ställ in WEP-nyckeln med formaten ASCII och HEX. Du kan skriva in kodtecken för ASCII (5 eller 13 ASCII-tecken. Otillåtna tecken som t.ex. ”/” får inte användas.) eller 10/26 HEX-tecken.
- **Standardnyckel:** Välj en av de fyra konfigurerade nycklarna som den för tillfället tillgängliga.

6.2.2 WPA-personlig

WPA (Wi-Fi Protected Access), en wifi-standard, är ett nyare trådlöst krypteringssystem för att förbättra WEP:s säkerhetsfunktioner. Det tillämpar kraftfullare krypteringstyper (som t.ex.TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]) och kan funktionellt ändra alla behöriga trådlösa anordningars nycklar.

- **Välj SSID:** Välj SSID (huvudsakliga SSID eller andra SSID) för att konfigurera säkerhetsinställningar från rullgardinsmenyn.
- **WPA-algoritmer:** Tillhandahåller TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standard är TKIP-läge.
- **Lösenfras:** Skriv in de krypterade tecknen med 8-63 ASCII-tecken.
- **Nyckeländringsintervall:** Ställ in nyckelns förnyelseperiod.

6.2.3 WPA2-personlig

WPA2 (Wi-Fi Protected Access version 2) ger högre säkerhet än WEP (Wireless Equivalent Privacy) och WPA (Wi-Fi Protected Access).

- **Välj SSID:** Välj SSID (huvudsakliga SSID eller andra SSID) för att konfigurera säkerhetsinställningar från rullgardinsmenyn.
- **WPA-algoritmer:** Tillhandahåller TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standard är TKIP-läge.

- **Lösenfras:** Skriv in de krypterade tecknen med 8-63 ASCII-tecken.
- **Nyckeländringsintervall:** Ställ in nyckelns förnyelseperiod.

6.2.4 WPA-företag

Detta säkerhetsläge används när en RADIUS-server är ansluten till anordningen. Välj ”WPA-företag” från rullgardinsmenyn för att gå till följande fönster.

- **Välj SSID**: Välj SSID (huvudsakliga SSID eller andra SSID) för att konfigurera säkerhetsinställningar från rullgardinsmenyn.
- **WPA-algoritmer**: Tillhandahåller TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standard är TKIP-läge.
- **Nyckeländringsintervall:** Ställ in nyckelns förnyelseperiod.
- **Radius-server:** Skriv in Radius-serverns IP-adress.
- **Radius-serverns port:** Skriv in Radius-serverns autentiseringsport. Standard är 1812.
- **Delad hemlighet:** Skriv in den delade nyckeln för autentiseringsservern med 8 ... 63 ASCII-tecken.
- **Time-out för session:** Autentiseringsintervallsperiod mellan AP och autentiseringsserver.

6.2.5 WPA2-företag

Detta säkerhetsläge baseras på Radius autentiseringsserver och WPA2 datakrypteringstyp. WPA2 används när en RADIUS-server är ansluten till anordningen. Välj ”WPA2-företag” från rullgardinsmenyn för att gå till följande fönster.

- **Välj SSID:** Välj SSID (huvudsakliga SSID eller andra SSID) för att konfigurera säkerhetsinställningar från rullgardinsmenyn.
- **WPA-algoritmer:** Tillhandahåller TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standard är TKIP-läge.
- **Nyckeländringsintervall:** Ställ in nyckelns förnyelseperiod.
- **Radius-server:** Skriv in Radius-serverns IP-adress.
- **Radius-serverns port:** Skriv in Radius-serverns autentiseringsport. Standard är 1812.
- **Delad hemlighet:** Skriv in den delade nyckeln för autentiseringsservern med 8 ... 63 ASCII-tecken.
- **Time-out för session:** Autentiseringsintervallsperiod mellan AP och autentiseringsserver. Standard är 3600 s.

6.2.6 802.1X

Detta säkerhetsläge används när en RADIUS-server är ansluten till anordningen. 802.1x, ett slags portbaserat autentiseringsprotokoll, är en autentiseringstyp och strategi för användare. Porten kan antingen vara fysisk eller logisk (som t.ex. VLAN). För användare av trådlöst LAN är en port endast en kanal. Syftet med 802.11x-autentisering är att kontrollera om porten kan användas. Om porten autentiseras kan du öppna den och därmed tillåts alla meddelanden att passera. Om porten inte autentiseras kan den stå kvar som ”inaktiverad” och då tillåts endast meddelanden från autentiseringsprotokoll 802.1x att passera. Välj ”802. 1x” från rullgardinsmenyn för att gå till följande fönster.

- **Välj SSID:** Välj SSID (huvudsakliga SSID eller andra SSID) för att konfigurera säkerhetsinställningar från rullgardinsmenyn.
- **WEP:** Klicka på ”Aktivera/Inaktivera” för att aktivera eller inaktivera WEP-algoritmen.
- **Radius-server:** Skriv in Radius-serverns IP-adress.
- **Radius-serverns port:** Skriv in Radius-serverns autentiseringsport. Standard är 1812.
- **Delad hemlighet:** Skriv in den delade nyckeln för autentiseringsservern med 8 ... 63 ASCII-tecken.
- **Time-out för session:** Autentiseringsintervallsperiod mellan AP och autentiseringsserver. Standard är 3600 s.

6.4 Inställningar för WPS

WPS (Wi-Fi Protected Setting) kan användas för att enkelt och snabbt upprätta anslutningen mellan de trådlösa nätverkens klienter och anordningen via krypterat innehåll. Användarna skriver endast in en PIN-kod eller trycker på knappen WPS på panelen för att konfigurera det utan att manuellt välja en datakrypteringstyp eller hemliga nycklar. I menyn ”Trådlösa inställningar” klickar du på ”WPS-inställningar” för att komma till nästa skärm.

- **WPS-inställningar:** Aktivering eller inaktivering av WPS-funktionen. Standard är ”inaktivera”.
- **WPS-läge:** Ger två möjligheter: PBC (Push-Button Configuration) eller PIN-kod.
- **PBC:** Välj PBC eller tryck på knappen WPS på anordningens främre panel i ca en sekund (Tryck på knappen i ca en sekund och WPS-indikatorn blinkar i 2 minuter, vilket visar att WPS är aktiverat. Medan det blinkar, kan du aktivera en annan anordning så att WPS/PBC-sökningen mellan dem genomförs. Efter två minuter stängs WPS-indikatorn av, vilket innebär att WPS-anslutningen avslutats. Om fler klienter läggs till upprepas stegen ovan. För närvarande stöder WPS åtkomst för upp till 32 klienter.).
- PIN: Om detta val är aktiverat måste du föra in en trådlös klients PIN-kod i fältet och behålla samma kod i WPS-klienten.

6.5 Inställningar för WPS

WDS (Wireless Distribution System) används för att utöka den trådlösa täckningsarean. Med denna router ges tre lägen: Lazy, brygga och repeater.

Lazy: I detta läget kan den anslutna anordningen vara i läget brygga eller repeater. Skriv in routerns BSSID för att upprätta anslutningen.

Brygga: Två eller fler fasta nätverk kan via detta läge anslutas trådlöst. I detta läge måste du lägga till den anslutande anordningens trådlösa MAC-adress till routerns tabell över AP MAC-adresser eller välja en från tabellscanningen.

Repeaterläge: I detta läge läggs den motsatta MAC-adressen till manuellt eller via scanner i varje tabell över AP MAC-adresser för att förstora och utvidga den trådlösa radion.

Kapitel 7: DHCP-server

7.1 Inställningar för DHCP

DHCP (Dynamic Host Control Protocol) tilldelar en IP-adress till datorerna i LAN/privat nätverk. När du aktiverar DHCP-servern, kommer den att automatiskt allokera en oanvänd IP-adress från poolen av IP-adresser till den dator som så begär förutsatt att ”Erhåll en IP-adress automatiskt” aktiverats. Därför måste start- och slutadress för IP-adressen anges.

- **DHCP-server:** Kryssa i rutan för att aktivera DHCP-servern.
- **IP-adressens start/slut:** Skriv in IP-adressens räckvidd för distribution via DHCP-server.
- **Leasingtid:** Tiden IP-adressen leasas.

Kapitel 8: Uppgradera inbyggda program

8.1 Det går att uppgradera routerns inbyggda program. Ladda ned paketet för uppgradering av inbyggda program från www.nedis.nl och klicka på ”Uppgradera” efter att du bläddrat igenom paketet.

- **Bläddra igenom**: Klicka på denna knapp för att välja uppgraderingsfil.
- **Uppgradera**: Klicka på denna knapp för att starta uppgraderingsprocessen. När uppgraderingen avslutas kommer routern att starta om automatiskt.

8.2 Starta om routern

Omstart av routern gör att de konfigurerade inställningarna träder i kraft eller så ställs routern in på nytt om inställningarna misslyckades.

8.3 Ändring av lösenord

Denna avdelning är för att ställa in ett nytt användarnamn och lösenord med högre säkerhet för routern och nätverket.

- **Användarnamn:** Skriv in ett användarnamn för anordningen.
- **Gammalt lösenord:** Skriv in det gamla lösenordet.
- **Nytt lösenord:** Skriv in ett nytt lösenord.
- **Skriv in det en gång till för att bekräfta:** Skriv in lösenordet en gång till för att bekräfta det.

8.4 Logga ut

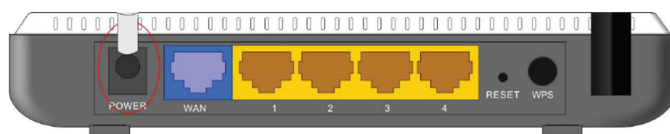
När du avslutat inställningarna klickar du på ”Ja” på utloggningssidan för att logga ut från administrationssidan på webben.

Hur du installerar och ställer in en router med ett kabel- eller ADSL-modem

Varning!

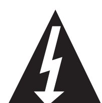
Följ dessa steg utan att hoppa över något steg

1. Stäng av modemet (koppla från elnätet).
2. Stäng av den stationära/bärbara datorn.
3. Anslut **LAN-utgången** på modemet med **LAN-kabel** till den **blå porten** på routern.
4. Anslut en av de **gula portarna** med **LAN-kabeln** till den stationära/bärbara datorn.



5. Slå nu på modemet och vänta tills det är helt inloggat (detta kan ta en stund).
6. Slå på routern och vänta i minst 30 sekunder.
7. Starta den stationära/bärbara datorn och vänta tills den är helt igångsatt.
8. Öppna din webbläsare och gå till http://192.168.0.1.
9. Ange användarnamn och lösenord (båda standard: **admin**).
10. Gå till **Inställningsguiden** och klicka på **Autoidentifiering**.
11. Klicka nu på **Nästa** och i följande ruta klickar du på Verkställ.
12. Gå till menyn **WLAN inställningar** och se till att **Aktivera trådlöst nätverk** är markerat.
13. Här kan du konfigurera ditt nätverksnamn (SSID) och kanalen.
14. Gå till undermenyn **Säkerhetsinställningar** och välj säkerhetstyp. Vi rekommenderar att alltid välja **Blandad WPA/WPA2 - Personlig**.
15. Välj **WPA Algoritmer** som **TKIP&AES**.
16. Ändra lösenordet i fältet **Lösenordsfras**. Vi rekommenderar att välja ett starkt lösenord som består av bokstäver, siffror och eventuellt 1 eller flera specialtecken.
17. Klicka på **Verkställ** för att spara informationen.
18. Avsluta webbläsaren; ditt trådlösa nätverk och dina säkerhetsinställningar är nu klara. Du kan även koppla bort kabeln mellan routern och stationära/bärbara datorn för att upprätta en trådlös anslutning (om datorn är utrustad med en trådlös mottagare).

Säkerhetsanvisningar:






För att minska risken för elektriska stötar bör denna produkt ENDAST öppnas av behörig tekniker när service behövs. Dra ut strömkabeln från eluttaget och koppla ur all annan utrustning om något problem skulle uppstå. Utsätt inte produkten för vatten eller fukt.

Underhåll:
Rengör endast med torr trasa. Använd inga rengöringsmedel som innehåller lösningsmedel eller slipmedel.

Garanti:
Ingen garanti gäller vid ändringar eller modifieringar av produkten eller för skador som har uppstått på grund av felaktig användning av denna produkt.

Allmänt:
- Utseende och specifikationer kan komma att ändras utan föregående meddelande.
- Alla logotyper och produktnamn är varumärken eller registrerade varumärken som tillhör sina ägare och är härmed erkända som sådana.
- Den här bruksanvisningen producerades med omsorg. Dock kan inga rättigheter härröra. König Electronic kan inte acceptera ansvar för några felaktigheter i denna manual eller dess konsekvenser.
- Behåll bruksanvisningen och förpackningen för eventuellt framtida behov.

Obs!

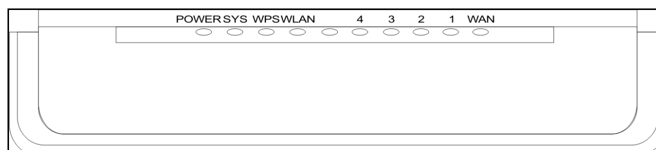
Produkten är märkt med denna symbol som betyder att använda elektriska eller elektroniska produkter inte får slängas bland vanliga hushållssopor. Det finns särskilda återvinningssystem för dessa produkter.

ČESKY

Kapitola 1 Popis

1.1 Popis LED indikátorů a portů

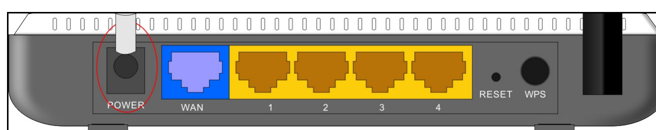
Přední panel a zobrazení LED indikátorů



Popis LED indikátorů na předním panelu (zleva doprava)

- **POWER (napájení)**
  Svítící zelená LED signalizuje, že je router správně napájen.
- **SYS**
  Blikající zelená LED signalizuje správnou funkci systému.
- **WPS**
  Jestliže bliká, znamená to, že zařízení komunikuje s klientem ve WPS režimu.
- **WLAN**
  LED indikátor bezdrátového signálu. Jestliže zelená LED bliká, je aktivována bezdrátová funkce.
- **LAN (4, 3, 2, 1)**
  LED indikátor lokální kabelové sítě. Jestliže svítí, router je připojen do Ethernetu. Blikání indikuje odesílání a/nebo přijímání dat.
- **WAN**
  Indikátor bezdrátové počítačové sítě. Pokud svítí, je bezdrátová síť zapnuta.

Zobrazení zadního panelu:



Zadní panel: (zleva doprava)

- **POWER (napájení)**

Konektor pro připojení napájecího adaptéru. Použijte prosím 9 V DC adaptér, který je součástí výrobku.

- **WAN**

100 Mbps port Ethernetu, který může být připojen k MODEMU, přepínači, routeru a k dalším ethernetovým zařízením určeným pro připojení k Internetu pomocí DSL MODEMU, kabelového MODEMU a ISP (poskytovatel připojení k internetu).

- **LAN (1, 2, 3, 4)**

Čtyři 10/100 Mbps ethernetové porty, které mohou být připojeny k přepínači, routeru a NIC (síťová karta)

- **RESET**

Tlačítko resetování systému. Přidržte toto tlačítko 7 sekund - dojde k vymazání konfigurovaných nastavení a obnově standardního nastavení.

- **WPS**

Stiskněte jej na 1 sekundu, WPS funkce bude aktivována a WPS indikátor bude blikat.

Kapitola 2: Instalace hardware

2.1 Jak provést instalaci routeru

K napájení routeru prosím použijte dodaný napájecí adaptér. DŮLEŽITÉ: Při použití jiného napájecího adaptéru může dojít k poškození a zániku záruky na tento výrobek. Připojte prosím LAN port routeru k síťovému adaptéru vašeho počítače pomocí kabelu. Připojte prosím širokopásmovou linku poskytnutou vaším ISP (poskytovatel připojení k internetu) k WAN portu. Vložte dodaný CD-ROM do mechaniky, dvakrát klikněte na ikonu „Setup“ (nastavení) a řiďte se instrukcemi pro dokončení instalace. Nebo můžete navštívit webovou stránku routeru k jeho konfiguraci. (Více podrobností je uvedeno v kapitole 3)

Kapitola 3: Jak se přihlásit k routeru

3.1 Jak nastavit konfiguraci sítě

1. Na pracovní ploše vašeho počítače klikněte pravým tlačítkem myši na „Místa v síti“ a zvolte „Vlastnosti“.
2. Klikněte pravým tlačítkem myši na „Připojení k místní síti“ a zvolte „Vlastnosti“.
3. Zvolte „Internetový protokol (TCP/IP)“ a klikněte na „Vlastnosti“.
4. - Zvolte „Získat IP adresu automaticky“ a „Získat adresu DNS serveru automaticky“. Klikněte na „OK“ k uložení konfigurace.
   - Nebo zvolte položku „Použít následující IP adresu“ a vložte IP adresu, masku podsítě a výchozí bránu následovně: IP adresa: 192.168.0.XXX: (XXX je číslo v rozsahu 2 - 254) Maska podsítě: 255.255.255.0. Brána: 192.168.0.1. Musíte vložit adresu DNS serveru poskytnutou vaším ISP (poskytovatel připojení k internetu) Jinak můžete použít výchozí bránu routeru jako DNS proxy server. Klikněte na „OK“ k uložení konfigurace.

3.2 Přihlášení k routeru

1. K přístupu do webového rozhraní routeru spusťte webový prohlížeč jako je Internet Explorer nebo Firefox a vložte výchozí IP adresu routeru - http://192.168.0.1. Stiskněte „Enter“.
2. Do obou polí uživatelského jména a hesla vložte „admin“. Klikněte na „OK“.

Výchozí nastavení	
IP adresa	192.168.0.1
Heslo	admin
SSID	KONIG
Režim zabezpečení	Deaktivován
Bezdrátový režim	b/g/n smíšený režim
Kanál	Automatický výběr
Časová zóna	
WPS nastavení	aktivováno
Název zařízení UPNP	11N Wireless Broadband Router
Výrobce UPNP	KONIGELECTRONIC
Název modelu UPNP	CMP-WNROUT41
Číslo modelu UPNP	V 1.0
Udaná síťová rychlost UPNP	300 Mbps
Adresa zařízení UPNP	http://192.168.0.1
UPNP	Deaktivován

Kapitola 4: Průvodce rychlým nastavením

4.1 Průvodce nastavením

Pro rychlou konfiguraci routeru se objeví zpráva „Welcome to Setup Wizard“ (Vítejte v průvodci nastavením) klikněte na „Next“ (další)

V této obrazovce vyberte jeden režim Internetového připojení, které používáte. Jestliže si nejste jisti stiskněte tlačítko „Detect“ (detekce) nebo kontaktujte svého poskytovatele internetu a klikněte na „Next“ (další).

Virtuální vytáčení ADSL (přes PPPoE)

Vstupte do účtu a vložte heslo poskytnuté vaším ISP (poskytovatel připojení k internetu) a klikněte na „Next“ (další).

Dynamická IP (přes DHCP)

Je-li vaším režimem připojení dynamická IP znamená to, že se po každém připojení změní. Nemusíte vkládat informace jako je tomu u jiných režimů. Klikněte na „Next“ (další) a „Save“ (uložit) k ukončení nastavení.

Statická IP

V této obrazovce vložte informaci o síťové adrese od vašeho ISP (poskytovatel připojení k internetu) jako je IP adresa, maska podsítě, brány a vyplňte pole primárního DNS serveru a klikněte na „Next“ (další).

L2TP

K získání požadované informace kontaktujte svého ISP (poskytovatel připojení k internetu).

Kapitola 5: Pokročilá nastavení

5.1 Nastavení LAN

LAN konfigurace nastavuje základní parametry TCP/IP LAN portů.

- **IP adresa:** IP adresy LAN routeru (ne IP adresa vašeho PC) Standardní hodnotou je 192.168.0.1.
- **Maska podsítě:** Zobrazuje masku pro rozdělení podsítě routeru. Základní hodnotou je 255.255.255.0.

DŮLEŽITÉ:

Po změně IP adresy je nutno si ji zapamatovat k příštímu přihlášení do webového rozhraní.

5.2 Nastavení WAN

Jakmile si v „Setup Wizard“ (průvodci nastavení) zvolíte typ ISP připojení a budete chtít změnit příslušná nastavení můžete tyto změny a konfiguraci provést podrobně zde.

Statická IP

Je-li jako režim připojení zvolena statická IP můžete změnit následující informaci o adrese.

- **IP adresa:** Zde vložte IP adresu WAN poskytnutou vaším ISP (poskytovatel připojení k internetu).
- **Maska podsítě:** Zde vložte masku podsítě WAN.
- **Mezisíťová brána:** Zde vložte mezisíťovou bránu WAN.
- **Primární DNS server:** Vložte primární DNS server poskytnutý vaším ISP.
- **Sekundární DNS server:** Vložte sekundární DNS.

Kapitola 6: Bezdrátové nastavení

6.1 Základní nastavení

- **Aktivace bezdrátového připojení:** Zaškrtněte pole k aktivaci bezdrátového připojení routeru, k jeho deaktivaci zrušte zaškrtnutí.
- **Síťový režim:** Vyberte jeden z následujících. Standardním režimem je 11b/g/n.
- **Hlavní SSID:** SSID (identifikace nastavení služeb) je specifický název bezdrátové sítě. Toto zařízení má dvě SSID - hlavní SSID je nezbytná.
- **Vedlejší SSID:** Je volitelná.

- **Vysílání (SSID):** Zvolte „Enable“ (aktivovat) k aktivaci SSID zařízení aby bylo viditelné pro bezdrátové klienty. Standardním nastavením je aktivace.
- **Izolace MBSSID přístupového bodu:** Řídící vlastnost jednoho přístupu je založena na bezdrátové MAC adrese. Je-li tato vlastnost aktivována, bezdrátoví klienti připojení ke stejné SSID nemohou mezi sebou komunikovat.
- **Izolace přístupového bodu:** Řídící vlastnost jednoho přístupu je založena na SSID. Je-li tato vlastnost aktivována, každý z vašich bezdrátových klientů bude na své vlastní virtuální síti a nebude možno vzájemně komunikovat. Je-li tato vlastnost aktivována, bezdrátoví klienti připojení k hlavní SSID a vedlejší SSID spolu nemohou vzájemně komunikovat což pomůže velmi zabezpečit bezdrátovou síť.
- **Kanál:** Specifikujte efektivní kanál (od 1 do 13/auto) bezdrátové sítě.
- **Rozšiřující kanál:** K zvýšení průchodnosti dat bezdrátové sítě se rozšiřující kanál používá v režimu 11n.
- **Šířka pásma kanálu:** Ke zlepšení bezdrátového přenosu zvolte šířku pásma kanálu. Jestliže má síť 11b/g a 11n klienty můžete zvolit 40M, je-li síť 11n zvolte 20/40M k zvýšení průchodnosti dat.

6.2 Nastavení zabezpečení bezdrátové sítě

Používá se ke konfiguraci nastavení bezpečnosti AP (přístupový bod) sítě. Toto zařízení disponuje šesti (celkem deseti) běžnými kódovacími metodami včetně Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise apod..

6.2.1 Mixed WEP (smíšený WEP)

WEP (soukromí ekvivalentní kabelovým sítím) je základní kódovací metodou obyčejně používanou ke kódování bezdrátových dat pomocí série digitálních klíčů (64 bitových nebo 128 bitových) Použitím stejných klíčů na každé z vašich bezdrátových síťových zařízení můžete zabránit jejich monitorování nebo vysílání či využití vašich bezdrátových zdrojů. Zvolte Mixed WEP ke vstupu do následujícího okna:

- **Volba SSID:** Zvolte SSID (hlavní nebo vedlejší SSID) ke konfiguraci zabezpečení z rozbalovacího seznamu.
- **Režim zabezpečení:** Z rozbalovacího seznamu zvolte příslušný kódovací režim.
- **WEP klíč 1~4**: Nastavte WEP klíč pomocí ASCII nebo hex soustavě. Můžete vložit ASCII kód (5 nebo 13 ASCII znaků. Neplatné znaky jako je „/“ nejsou povoleny) nebo 10/26 hex znaků.
- **Standardní klíč:** Zvolte jeden klíč ze čtyř konfigurovaných jako aktuální.

6.2.2 WPA-Personal

WPA (Wi-Fi chráněný přístup) je Wi-Fi je standardem a nejnovější bezdrátové kódovací schéma vyvinuté k zlepšení vlastností zabezpečení WEP. Používá mocnější kódovací typy (jako je TKIP [temporální protokol integrity klíče] nebo AES [zdokonalený standard kódování]) a může dynamicky měnit klíče na každém autorizovaném bezdrátovém zařízení.

- **Volba SSID:** Zvolte SSID (hlavní nebo vedlejší SSID) ke konfiguraci zabezpečení z rozbalovacího seznamu.
- **WPA algoritmy:** Poskytuje TKIP [temporální protokol integrity klíče] a AES [zdokonalený standard kódování]. Standardním režimem je TKIP.
- **Vložení fráze:** Vložte kódovací znaky za pomocí 8 - 63 ASCII znaků.
- **Interval obnovy klíče:** Nastavte interval obnovy klíče.

6.2.3 WPA2- Personal

WPA2 (chráněný přístup k Wi-Fi verze 2) poskytuje větší zabezpečení než WEP (bezdrátové ekvivalentní soukromí) a WPA (Wi-fi chráněný přístup).

- **Volba SSID:** Zvolte SSID (hlavní nebo vedlejší SSID) ke konfiguraci zabezpečení z rozbalovacího seznamu.
- **WPA algoritmy:** Poskytuje TKIP [temporální protokol integrity klíče] a AES [zdokonalený standard kódování]. Standardním režimem je TKIP.

- **Vložení fráze:** Vložte kódovací znaky za pomocí 8 - 63 ASCII znaků.
- **Interval obnovy klíče:** Nastavte interval obnovy klíče.

6.2.4 WPA- Enterprise

Tento zabezpečovací režim se používá je-li k zařízení připojen RADIUS server. Zvolte z rozbalovacího seznamu „WPA-Enterprise“ ke vstupu do následujícího okna.

- **Volba SSID:** Zvolte SSID (hlavní nebo vedlejší SSID) ke konfiguraci nastavení zabezpečení z rozbalovacího seznamu.
- **WPA Algoritmy**: Poskytují TKIP [temporální protokol integrity klíče] nebo AES [zdokonalený standard kódování]. Standardním režimem je TKIP.
- **Interval obnovy klíče:** Nastavte interval obnovy klíče.
- **Server Radius:** Vložte IP adresu serveru Radius.
- **Port serveru Radius:** Vložte autentizační port serveru Radius. Standardním portem je 1812.
- **Sdílený klíč:** Vložte sdílený klíč pro autentizační server v rozmezí 8 - 63 ASCII znaků.
- **Doba vypršení relace:** Je autentizačním intervalem mezi přístupovým bodem a autentizačním serverem.

6.2.5 WPA2-Enterprise

Tento zabezpečovací režim je založen na autentizačním serveru Radius a kódovací metodě WPA2. WPA2 se používá, jestliže je k zařízení připojen server RADIUS. Zvolte „WPA2-Enterprise“ z rozbalovacího seznamu ke vstupu do následujícího okna.

- **Volba SSID:** Zvolte SSID (hlavní nebo vedlejší SSID) ke konfiguraci zabezpečení z rozbalovacího seznamu.
- **WPA algoritmy:** Poskytuje TKIP [temporální protokol integrity klíče] a AES [zdokonalený standard kódování]. Standardním režimem je TKIP.
- **Interval obnovy klíče:** Nastavte interval obnovy klíče.
- **Server Radius:** Vložte IP adresu serveru Radius.
- **Port serveru Radius:** Vložte autentizační port serveru Radius. Standardním portem je 1812.
- **Sdílený klíč:** Vložte sdílený klíč pro autentizační server v rozmezí 8 - 63 ASCII znaků.
- **Doba vypršení relace:** Je autentizačním intervalem mezi přístupovým bodem a autentizačním serverem. Standardním intervalem je 3 600 s.

6.2.6 802.1X

Tento zabezpečovací režim se používá je-li k zařízení připojen RADIUS server. 802.1X je autentizačním protokolem na bázi portu, který je autentizačním typem a strategií pro uživatele. Portem může být fyzický port nebo logický port (jako např. VLAN). Pro uživatele bezdrátové LAN je portem kanál. Hlavním účelem autentizace 802.11x je zjistit jestli může být port použit. Jestliže je port úspěšně autentizován můžete ho otevřít což umožní aby jím procházely všechny zprávy. Jestliže není port úspěšně autentizován můžete ho mít „disabled“ (deaktivovaný) a budou jím procházet pouze zprávy 802.1x autentizačního protokolu. Vyberte z rozbalovacího seznamu „802.1x“ ke vstupu do následujícího okna.

- **Volba SSID:** Zvolte SSID (hlavní nebo vedlejší SSID) ke konfiguraci zabezpečení z rozbalovacího seznamu.
- **WEP**: Klikněte na „Enable/Disable“ (aktivovat/deaktivovat) k aktivaci/deaktivaci WEP algoritmu.
- **Server Radius:** Vložte IP adresu serveru Radius.
- **Port serveru Radius:** Vložte autentizační port serveru Radius. Standardním portem je 1812.
- **Sdílený klíč:** Vložte sdílený klíč pro autentizační server v rozmezí 8 - 63 ASCII znaků.
- **Doba vypršení relace:** Je autentizačním intervalem mezi přístupovým bodem a autentizačním serverem. Standardním intervalem je 3 600 s.

6.4 WPS nastavení

WPS (zabezpečené nastavení Wi-fi) může být použito k snadnému a rychlému navázání spojení mezi klienty bezdrátové sítě a zařízením s kódovaným obsahem. Uživatelé pouze vloží PIN kód nebo stisknou tlačítko WPS k jeho konfiguraci bez ručního výběru kódovací metody a tajných klíčů. V nabídce „Wireless settings“ (bezdrátová nastavení) klikněte na „WPS settings“ (WPS nastavení) ke vstupu do další obrazovky.

- **WPS nastavení:** Aktivace a deaktivace WPS funkce. Standardním nastavení je „disable“ (deaktivace).
- **WPS režim:** Poskytuje dvě metody: PBC (konfiguraci tlačítka) a PIN kód.
- **PBC**: Zvolte PBC nebo stiskněte tlačítko WPS na předním panelu zařízení asi na jednu sekundu (při stisku tlačítka na jednu sekundu bude indikátor WPS blikat 2 minuty což znamená, že je WPS aktivováno). Při blikajícím indikátoru můžete aktivovat další zařízení k implementaci WPS/PBC mezi nimi. Po dvou minutách WPS indikátor zhasne a to znamená, že je WPS připojení dokončeno. K přidání více klientů opakujte výše uvedené kroky. V této době WPS podporuje přístup až 32 klientů.
- PIN: Je-li aktivována tato volba je nutno zadat do pole PIN kód bezdrátového klienta a stejný kód musí obsahovat WPS klient.

6.5 WDS nastavení

WDS (bezdrátový distribuční systém) se používá k rozšíření oblasti bezdrátového pokrytí. Tento router poskytuje tři režimy: Lazy, Bridge a Repeater.

Lazy: U tohoto režimu může být připojené zařízení v přemostěném režimu nebo v režimu repeateru a může vstoupit do BSSID routeru k navázání spojení.

Bridge: Pomocí tohoto režimu můžete bezdrátově připojit dvě nebo více kabelových sítí. V tomto režimu je zapotřebí přidat bezdrátovou MAC adresu připojovaného zařízení do tabulky MAC adres přístupových bodů routeru nebo vybrat jeden z tabulky vyhledávání zařízení.

Repeater: V tomto režimu přidejte ručně protisměrnou MAC adresu do každé vlastní tabulky MAC adres přístupového bodu nebo pomocí vyhledávání k rozšíření bezdrátové sítě.

Kapitola 7: DHCP Server

7.1 DHCP nastavení

DHCP (dynamický konfigurační protokol klienta v počítačové síti) přiřazuje IP adresu počítačům na LAN/privátní síti. Po aktivaci DHCP serveru tento automaticky přiřadí nepoužité IP adresy žádajícímu počítači za předpokladu označení položky „Obtain IP Address Automatically“ (Získat adresu IP automaticky). Je zapotřebí specifikace počáteční a konečné adresy ze seznamu nepoužitých IP adres.

- **DHCP Server**: Označte zaškrtávací pole k aktivaci DHCP serveru.
- **Počátek/konec IP adresy:** K distribuci adres DHCP serverem vložte rozsah IP adresy.
- **Doba pronájmu:** Doba pronájmu IP adresy.

Kapitola 8: Upgrade Firmware

8.1 Router poskytuje upgrade firmware kliknutím na „Upgrade“ po vyhledání balíčku upgrade firmware, který si můžete stáhnout z www.nedis.nl.

- **Browse**: Klikněte na toto tlačítko k výběru souboru upgrade.
- **Upgrade**: Klikněte na toto tlačítko k započetí procesu upgrade. Po dokončení upgrade se router automaticky restartuje.

8.2 Restartování routeru

Při restartování routeru vstoupí v platnost konfigurovaná nastavení nebo jestliže selžou dojde k opětovnému nastavení routeru.

8.3 Změna hesla

V této části je popisováno vložení nového uživatelského jména a hesla k lepšímu zabezpečení routeru a sítě.

- **Uživatelské jméno:** Vložte pro zařízení nové uživatelské jméno.

- **Staré heslo:** Vložte staré heslo.
- **Nové heslo:** Vložte nové heslo.
- **Vložení nového hesla k potvrzení:** Vložte nové heslo pro potvrzení.

8.4 Odhlášení

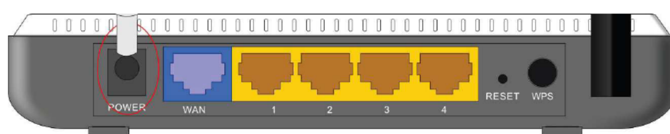
Po dokončení nastavení klikněte na „Yes“ na odhlašovací stránce k odhlášení z webové stránky nastavení.

Jak instalovat a nastavit router ke kabelu nebo modemu ADSL

Upozornění!

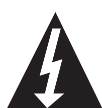
Posupujte podle jednotlivých kroků Jednotlivé kroky není možné přeskakovat

1. Vypněte modem (odpojte jej z napájení).
2. Vypněte své PC/notebook.
3. Připojte výstup **LAN modemu** přes **kabel LAN** k modrému **portu routeru.**
4. Připojte jeden ze **žlutých portů** přes **kabel LAN** ke svému PC/notebook.



5. Zapněte nyní modem a počkejte, až bude plně přihlášený (může to chvíli trvat).
6. Zapněte router a počkejte alespoň 30 sekund.
7. Nastartujte vaše PC/notebook a počkejte, až se úplně načte.
8. Otevřete váš prohlížeč a nasměrujte ho na http://192.168.0.1.
9. Vložte uživatelské jméno a heslo (obojí předem nastavené na: **admin**).
10. Přejděte ke spouštěcímu programu **Setup Wizzard** a klikněte na **Auto Detect** (automatické detekování).
11. Nyní klikněte na **Next/Další a** v následující obrazovce klikněte na **Apply/Použít.**
12. Běžte k menu **WLAN nastavení** a ujistěte se, že je dostupný **Wireless /bezdrátové připojení**).
13. Tady si můžete nakonfigurovat název vaší sítě (SSID) a kanál.
14. Běžte do podmenu **Bezpečnostní nastavení a** zvolte si bezpečnostní typ. Doporučujeme si vždy zvolit **Mixed WPA/WPA2 – Osobní**.
15. Zvolte **Algoritmy WPA/ WPA Algorithms** jako **TKIP&AES**.
16. V poli **Pass Phrase/Vložte heslo** změňte heslo. Doporučujeme volbu silného hesla, které se skládá z písmen, čísel a nejlépe 1 či vice zvláštních znaků.
17. K uschování dat klikněte na **Apply/Použít.**
18. Odejděte z obrazovky prohlížeče, Vaše bedrátová síť a bezpečnostní nastavení jsou nyní kompletní. K vytvoření bezdrátového připojení můžete rozpojit kabel mezi routerem a PC/notebookem (pokud je PC/notebook vybaven bezdrátovým přijímačem).

Bezpečnostní opatření:






Abyste snížili riziko úrazu elektrickým šokem, měl by být tento výrobek otevřen POUZE autorizovaným technikem, je-li to nezbytné. V případě, že dojde k závadě, odpojte výrobek ze sítě a od jiných zařízení. Výrobek nevystavujte vodě nebo vlhkosti.

Údržba:

K čištění používejte pouze suchý hadřík. Nepoužívejte čisticí rozpouštědla ani abrazivní prostředky.

Záruka:
Jakékoli změny, modifikace nebo poškození zařízení v důsledku nesprávného zacházení se zařízením ruší platnost záruční smlouvy.

Obecné upozornění:
- Design a specifikace výrobku mohou být změněny bez předchozího upozornění.
- Všechna loga a obchodní názvy jsou registrované obchodní značky příslušných vlastníků a jsou chráněny zákonem.
- Prestože manuál byl zpracován s maximalní péčí, tiskové chyby nejsou vyloučeny. Konig Electronic nepřebírá zodpovědnost za za škody vzniklé v souvislosti s chybami v manuálu.
- Pro budoucí použití uschovejte tento návod a obal.

Upozornění:



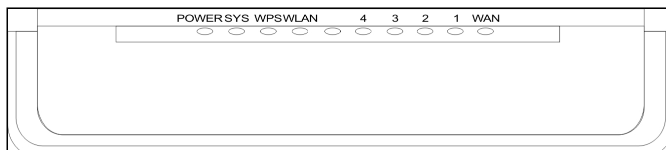
Tento výrobek je označen tímto symbolem. To znamená, že se s výrobkem musí zacházet jako s nebezpečným elektrickým a elektronickým odpadem a nelze jej po skončení životnosti vyhazovat s běžným domácím odpadem. Pro likvidaci těchto výrobků existují zvláštní sběrná střediska.

ROMÂNĂ

Capitolul 1: Introducere

1.1 Indicator LED şi descrierea porturilor

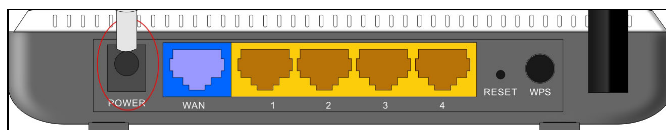
Panou frontal şi display al indicatorului LED



Descrierea indicatoarelor LED de pe panoul frontal: (de la stânga la dreapta)

- **POWER (ALIMENTARE ELECTRICITATE)**
  Atunci când beculețul verde rămâne aprins, acesta indică că cablul pentru alimentarea cu electricitate este conectat adecvat.
- **SYS (SISTEM)**
  Atunci când beculețul verde se aprinde intermitent, acesta indică că sistemul funcționează în mod adecvat.
- **WPS**
  Atunci când beculețul se aprinde intermitent, acesta indică că dispozitivul comunică cu clientul în modul WPS.
- **WLAN**
  Indicator LED al semnalului wireless. Atunci când beculețul verde se aprinde intermitent, acesta indică că funcția wireless este activată.
- **LAN (4, 3, 2, 1)**
  Indicator LED al rețelei locale prin cablu. Dacă beculețul rămâne aprins, acesta indică că dispozitivul este conectat la dispozitivul Ethernet; aprinderea intermitentă indică că dispozitivul transmite şi / sau primeşte date.
- **WAN**
  Indicatorul rețelei de zonă mare. Dacă beculețul rămâne aprins, acesta indică funcția wireless a router-ului.

Display-ul panoului din spate:



Panoul din spate: (de la stânga la dreapta)

- **POWER (ALIMENTARE ELECTRICITATE)**

Fişa jack este destinată conectării adaptorului pentru curentul electric. Vă rugăm să utilizați adaptorul de curent electric 9V CC furnizat.

- **WAN**

Un port Ethernet 100Mbps care poate fi conectat cu un MODEM, Switch, Router şi alte dispozitive Ethernet la DSL MODEM, MODEM prin cablu şi ISP (provider de Internet) pentru conexiunea la Internet.

- **LAN (1, 2, 3, 4)**

4 porturi Ethernet 10/100Mbps pot fi conectate cu switch Ethernet, router Ethernet şi card NIC.

- **RESET (RESETARE)**

Butonul de resetare a sistemului. Apăsați acest buton timp de 7 secunde, iar setările configurate în cadrul acestui dispozitiv vor fi anulate şi se va reveni la setările default, din fabrică.

■ **WPS**

Apăsaţi-l timp de 1 secundă, iar funcţia WPS va fi activată şi indicatorul WPS se va aprinde intermitent.

Capitolul 2: Instalarea hardware-ului

2.1 Modul de instalare a router-ului

Vă rugăm să utilizaţi adaptorul de curent electric furnizat pentru a alimenta cu electricitate router-ul. IMPORTANT: Utilizarea unui adaptor de curent electric diferit ar putea conduce la deteriorări şi ar putea face garanţia acestui dispozitiv nulă. Vă rugăm să conectaţi port-ul LAN al router-ului la adaptorul de reţea de la computer-ul dvs. cu ajutorul unui cablu. Vă rugăm să conectaţi cablul dvs. de bandă largă furnizat de ISP-ul dvs. la portul WAN. Introduceţi CD-ul furnizat în drive-ul CD-ROM-ului, faceţi dublu click pe icoana „Setup" (Instalare) şi urmaţi instrucţiunile pentru finalizarea instalării. Sau, puteţi accesa website-ul router-ului pentru a-l configura. (Pentru mai multe detalii, vă rugăm consultaţi Capitolul 3.)

Capitolul 3: Modul de logare la router

3.1 Modul de setare a configurărilor de reţea

1. Pe desktop-ul computerului dvs., faceţi click dreapta pe „My Network Places" (Locurile mele din reţea) şi selectaţi „Properties" (Proprietăţi).
2. Faceţi click dreapta pe „Local Area Network Connection" (Conexiune la Reţeaua Locală) şi selectaţi „Properties" (Proprietăţi).
3. Selectaţi „Internet Protocol (TCP/IP)" (Protocol Internet (TCP / IP) şi faceţi click pe „Properties" (Proprietăţi).
4. - Selectaţi „Obtain an IP address automatically" (Obţinerea automată a unei adrese IP) şi „Obtain DNS server address automatically" (Obţinerea automată a unei adrese de server). Click pe „OK" pentru a salva configurările.
   - Sau selectaţi „Use the following IP address" (Utilizaţi următoarea adresă IP) şi introduceţi adresa IP, Subnet mask şi Default gateway după cum urmează: IP Address (Adresa IP): 192.168.0.XXX: (XXX este un număr de la 2 la 254), Subnet Mask: 255.255.255.0., Gateway: 192.168.0.1. Trebuie să introduceţi neapărat adresa server-ului DNS furnizată de ISP-ul dvs. Altfel, puteţi utiliza codul default gateway al router-ului ca server proxy DNS. Click pe „OK" pentru a salva configurările.

3.2 Logare la router

1. Pentru a accesa interfaţa de Internet a router-ului, deschideţi un browser web, cum ar fi Internet Explorer sau Firefox, şi introduceţi adresa IP default a router-ului, http://192.168.0.1. Apăsaţi pe „Enter" (Introducere).
2. Introduceţi „admin" (Administrator) în căsuţele pentru User Name (Numele utilizatorului) şi Password (Parolă). Click pe „OK".

Setări default	
Adresa IP	192.168.0.1
Parola	Admin (Administrator)
SSID	KONIG
Mod securitate	Disable (Dezactivat)
Mod wireless	b/g/n Mixd Mode (Mod combinat b/g/n)
Canal	Autoselect (Selectare automată)
Fus orar	
Setări WPS	Enable (Activat)
Denumirea dispozitivului UPNP	11N Wireless Broadband Router (Router bandă largă wirless 11N)
Producător UPNP	KONIGELECTRONIC

Denumirea modelului UPNP	CMP-WNROUT41
Numărul modelului UPNP	V 1.0
Viteza raportată a rețelei UPNP	300Mbps
Adresa dispozitivului UPNP	http://192.168.0.1
UPNP	Disable (Dezactivat)

Capitolul 4: Ghid pentru instalare rapidă

4.1 Etape de instalare

Acesta este „Welcome to Setup Wizard" (Bun venit în etapele de instalare) pentru configurarea rapidă a router-ului dvs. Click pe „Next" (Următorul).

În această pagină, selectați un mod al conexiunii la Internet pe care îl utilizați. Dacă nu sunteți sigur, apăsați butonul „Detect" (Detectare) sau contactați-vă Provider-ul de Internet şi faceți click pe „Next" (Următorul).

Dial-up virtual ADSL (prin PPPoE)

Introduceți Contul şi Parola furnizate de ISP-ul dvs. şi faceți click pe „Next" (Următorul).

IP dinamic (prin DHCP)

Dacă modul dvs. de conectare este IP dinamic, înseamnă că adresa dvs. IP se modifică de fiecare dată când vă conectați la Internet. Nu trebuie să introduceți informațiile ca în cazul altor moduri. Click pe „Next" (Următorul) şi „Save" (Salvați) pentru a finaliza setările.

IP static

În această fereastră, introduceți informațiile adresei rețelei dvs. obținute de la ISP-ul dvs. în căsuțele IP Address (Adresa IP), Subnet Mask, Gateway şi Primary DNS server (server primar DNS) şi faceți click pe „Next" (Următorul).

L2TP

Cereți ISP-ului dvs. informațiile cerute în fereastră.

Capitolul 5: Setări avansate

5.1 Setări LAN

Setările LAN sunt destinate parametrilor fundamentali TCP / UP ai porturilor LAN.

- **IP Address (Adresa IP)**: Adresa IP a LAN-ului router-ului (nu adresa IP a PC-ului dvs.). 192.168.0.1 este codul default, din fabrică.
- **Subnet Mask**: Aceasta indică codul subnet mask a router-ului pentru cuantificarea dimensiunii rețelei. 255.255.255.0 este codul default, din fabrică.

IMPORTANT:

Odată ce ați modificat adresa IP, trebuie să o rețineți pentru următoarea logarea utilitară pe Internet.

5.2 Setările WAN

După ce ați selectat tipul conexiunii ISP din „Setup Wizard" (Kit instalare) şi doriți să modificați setările conexe, puteți modifica şi configura setările detaliate aici.

IP static

Dacă IP-ul static este ales ca mod de conectare, puteți modifica următoarele informații privitoare la adresă.

- **IP Address (Adresa IP)**: Introduceți aici adresa IP WAN furnizată de ISP-ul dvs.
- **Subnet Mask**: Introduceți aici WAN Subnet Mask.
- **Gateway**: Introduceți aici WAN Gateway.
- **Primary DNS Server (Server primar DNS)**: Introduceți aici codul Primary DNS server de ISP-ul dvs.
- **Secondary DNS Server (Server secundar DNS)**: Introduceți codul pentru DNS secundar.

Capitolul 6: Setări wireless

6.1 Setări de bază

- **Enable Wireless (Activare wireless)**: Verificați pentru activarea caracteristicilor wireless ale router-ului; debifați pentru dezactivarea acestora.
- **Network Mode (Mod rețea)**: Selectați un mod din următoarele. Modul default este modul 11b/g/n.
- **Main SSID (SSID principal)**: SSID (Cod Identificare Set Serviciu) este denumirea unică a rețelei wireless. Acest dispozitiv are două SSID-uri şi SSID principal este necesar.
- **Minor SSID (SSID minor)**: Acesta este opțional.
- **Broadcast (SSID)**: Selectați „Enable" (Activare) pentru a activa SSID-ul dispozitivului care va fi vizibil pentru clienții wireless. Setarea default este activată.
- **MBSSID AP Isolation (Izolare MBSSID AP)**: O caracteristică de control a accesului pe baza adresei wireless MAC. Atunci când această caracteristică este activată, clienții wireless conectați la acelaşi SSID nu pot comunica unul cu celălalt.
- **AP Isolation (Izolare AP)**: O caracteristică de controlul accesului pe baza SSID. Atunci când această caracteristică este activată, fiecare dintre clienții dvs. wireless se va afla în propria rețea virtuală şi aceştia nu vor putea să comunice între ei. Atunci când această caracteristică este activată, clienții wireless conectați la SSID Minor şi SSID Principal nu pot comunica unul cu celălalt, ceea ce poate asigura un grad mare de siguranță rețelei wireless.
- **Channel (Canal)**: Specifică canalul real (de la 1 la 13\Auto) al rețelei wireless.
- **Extension Channel (Canal Extindere)**: Pentru a majora randamentul de date al rețelei wireless, gama canalului extindere este utilizat în modul 11n.
- **Channel Bandwidth (Lățimea de bandă a Canalului)**: Selectați lățimea de bandă a canalului pentru a îmbunătăți performanțele wireless. Atunci când rețeaua are 11b/g şi 11n clienți, puteți selecta 40M; atunci când se află într-o rețea 11n, selectați 20/40M pentru a-i îmbunătăți randamentul.

6.2 Setări de securitate wireless

Acestea sunt utilizate pentru a configura setările de securitate ale rețelei AP. Aici sunt prezentate şase (dintre cele 10) metode de criptare cele mai obişnuite, inclusiv Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, etc.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy – Protejare Echivalentă Cablu), o metodă de criptare fundamentală, criptează, de obicei, datele wireless prin utilizarea unei serii de coduri digitale (64 bits sau 128 bits în lungime). Prin utilizarea aceloraşi coduri pentru fiecare dintre dispozitivele dvs. wireless, puteți împiedica dispozitivele wireless neautorizate de la monitorizarea transmisiunilor dvs. sau de la utilizarea resurselor dvs. wireless. Selectați Mixed WEP pentru a intra în următoarea fereastră:

- **Select SSID (Selectare SSID)**: Selectați SSID (SSID Principal sau SSID Minor) pentru a configura setările de securitate din meniul care se desfăşoară în jos.
- **Security Mode (Mod Securitate)**: Din meniul ce se desfăşoară în jos, selectați modurile de criptare pentru securitate corespunzătoare.
- **WEP Key1~4**: Setați codul WEP cu formatul ASCII şi Hex. Puteți introduce codul ASCII (5 sau 13 caractere ASCII. Caracterele nepermise ca „/" nu sunt acceptate.) sau 10/26 caractere.
- **Default Key (Cod default)**: Selectați un cod din cele patru coduri configurate spre a fi cel disponibil în prezent.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access, Acces Protejat Wi-Fi), un standard Wi-Fi, este o schemă de criptare wireless mai recentă, creată pentru a îmbunătăți caracteristicile de securitate ale WEP. Acesta utilizează tipuri de criptare mai puternice (cum ar fi TKIP [Temporal Key Integrity Protocol, Protocolul Integrității Codului

Temporal] sau AES [Advanced Encryption Standard, Standard Avansat de Criptare]) şi poate modifica codurile dinamic, pentru fiecare dispozitiv wireless autorizat.

- **Select SSID (Selectare SSID)**: Selectaţi SSID (SSID Principal sau SSID Minor) pentru a configura setările de securitate din meniul care se desfăşoară în jos.
- **WPA Algorithms (Algoritme WPA)**: Furnizează TKIP [Temporal Key Integrity Protocol] sau AES [Advanced Encryption Standard]. Modul default este TKIP.
- **Pass Phrase (Parola)**: Introduceţi caracterele criptate cu caractere 8-63 ASCII.
- **Key Renewal Interval (Interval de Reînnoire Code)**: Setaţi perioada de reînnoire cod.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2 - Acces Protejat Wi-Fi, versiunea 2) furnizează o securitate mai mare decât WEP (Wireless Equivalent Privacy) şi WPA (Wi-Fi Protected Access).

- **Select SSID (Selectare SSID)**: Selectaţi SSID (SSID Principal sau SSID Minor) pentru a configura setările de securitate din meniul care se desfăşoară în jos.
- **WPA Algorithms (Algoritme WPA)**: Furnizează TKIP [Temporal Key Integrity Protocol] sau AES [Advanced Encryption Standard]. Modul default este TKIP.
- **Pass Phrase (Parola)**: Introduceţi caracterele criptate cu caractere 8-63 ASCII.
- **Key Renewal Interval (Interval de Reînnoire Code)**: Setaţi perioada de reînnoire cod.

6.2.4 WPA- Enterprise

Acest mod de securitate este utilizat atunci când un server RADIUS este conectat la dispozitiv. Selectaţi „WPA-Enterprise" din meniul care se desfăşoară în jos pentru a intra în următoarea fereastră:

- **Select SSID (Selectare SSID)**: Selectaţi SSID (SSID Principal sau SSID Minor) pentru a configura setările de securitate din meniul care se desfăşoară în jos.
- **WPA Algorithms (Algoritme WPA)**: Furnizează TKIP [Temporal Key Integrity Protocol] sau AES [Advanced Encryption Standard]. Modul default este TKIP.
- **Key Renewal Interval (Interval de Reînnoire Code)**: Setaţi perioada de reînnoire cod.
- **Radius Server (Server Radius)**: Introduceţi adresa IP a serverului Radius.
- **Radius Server port (Portul Serverului Radius)**: Introduceţi portul de autentificare a serverului Radius. Portul default este 1812.
- **Shared Secret (Secret partajat)**: Introduceţi codul partajat pentru serverul de autentificare, cu 8~63 ASCII caractere.
- **Session Timeout (Expirare timp Sesiune)**: Perioada intervalului de autentificare între AP şi serverul de autentificare.

6.2.5 WPA2-Enterprise

Acest mod de securitate se bazează pe serverul de autentificare Radius şi metoda de criptare WPA2. WPA2 este utilizat atunci când un server RADIUS este conectat la dispozitiv. Selectaţi „WPA2-Enterprise" din meniul care se desfăşoară în jos pentru a intra în următoarea fereastră:

- **Select SSID (Selectare SSID)**: Selectaţi SSID (SSID Principal sau SSID Minor) pentru a configura setările de securitate din meniul care se desfăşoară în jos.
- **WPA Algorithms (Algoritme WPA)**: Furnizează TKIP [Temporal Key Integrity Protocol] sau AES [Advanced Encryption Standard]. Modul default este TKIP.
- **Key Renewal Interval (Interval de Reînnoire Code)**: Setaţi perioada de reînnoire cod.
- **Radius Server (Server Radius)**: Introduceţi adresa IP a serverului Radius.
- **Radius Server port (Portul Serverului Radius)**: Introduceţi portul de autentificare a serverului Radius. Portul default este 1812.
- **Shared Secret (Secret partajat)**: Introduceţi codul partajat pentru serverul de autentificare, cu 8~63 ASCII caractere.

- **Session Timeout (Expirare timp Sesiune)**: Perioada intervalului de autentificare între AP şi serverul de autentificare. Valoarea default este 3600s.

6.2.6 802.1X

Acest mod de securitate este utilizat atunci când un server RADIUS este conectat la dispozitiv. 802.1x, un tip de protocol de autentificare pe bază de port, este un tip şi o strategie de autentificare pentru utilizatori. Portul poate fi un port fizic sau un port logic (cum ar fi VLAN). Pentru utilizatorii LAN wireless, un port este doar un canal. Scopul final al autentificării 802.11x este de a verifica dacă portul poate fi utilizat. Dacă portul este autentificat cu succes, puteți deschide acest port care va permite tuturor mesajelor să fie transmise. Dacă portul nu este autentificat cu succes, puteți menține acest port „disabled” (dezactivat), ceea ce va permite doar ca mesajele protocolului de autentificare 802.1x să fie transmise. Selectați „802.1x” din meniul de desfăşurare în jos pentru a intra în următoarea fereastră:

- **Select SSID (Selectare SSID)**: Selectați SSID (SSID Principal sau SSID Minor) pentru a configura setările de securitate din meniul care se desfăşoară în jos.
- **WEP**: Click pe „Enable/Disable” (Activare / Dezactivare) pentru a activa sau dezactiva algoritmul WEP.
- **Radius Server (Server Radius)**: Introduceți adresa IP a serverului Radius.
- **Radius Server port (Portul Serverului Radius)**: Introduceți portul de autentificare a serverului Radius. Portul default este 1812.
- **Shared Secret (Secret partajat)**: Introduceți codul partajat pentru serverul de autentificare, cu 8~63 ASCII caractere.
- **Session Timeout (Expirare timp Sesiune)**: Perioada intervalului de autentificare între AP şi serverul de autentificare. Valoarea default este 3600s.

6.4 Setări WPS

WPS (Wi-Fi Protected Setting – Setare Protejată Wi-Fi) poate fi utilizat pentru a stabili rapid şi uşor conexiunea dintre clienții rețelei wireless şi dispozitiv prin intermediul conținuturilor criptate. Utilizatorii vor introduce doar un cod PIN sau vor apăsa pe butonul WPS de pe panou pentru a-l configura fără selectarea manuală a unei metode de criptare şi a codurilor secrete. În meniul „Wireless settings” (Setări wireless), faceți click pe „WPS settings” (Setări WPS) pentru a intra în următoarea secțiune.

- **WPS settings (Setări WPS)**: Pentru a activa sau dezactiva funcția WPS. Setarea default este „disable” (dezactivat).
- **WPS mode (Modul WPS)**: Furnizează două moduri: PBC (Push-Button Configuration – Configurare Apăsare Buton) şi codul PIN.
- **PBC**: Selectați PBC sau apăsați butonul WPS de pe panoul frontal al dispozitivului timp de aproximativ o secundă (Apăsați butonul timp de aproximativ o secundă şi indicatorul WPS se va aprinde intermitent timp de 2 minute, ceea ce înseamnă că WPS este activat. În timp ce acesta se aprinde intermitent, puteți activa un alt dispozitiv pentru implementarea negocierii WPS/PBC între acestea. După două minute, indicatorul WPS se va opri, ceea ce înseamnă că conexiunea WPS este finalizată. Dacă mai mulți clienți sunt adăugați, repetați etapele de mai sus. În prezent, WPS acceptă accesul unui număr de până la 32 clienți.)
- PIN: Dacă această opțiune este activată, trebuie să introduceți codul PIN al unui client wireless în câmp şi să păstrați acelaşi cod în cadrul clientului WPS.

6.5 Setări WDS

WDS (Wireless Distribution System – Sistemul de Distribuție Wireless) este utilizat pentru a extinde zona de acoperire wireless. Acest router asigură trei moduri: Lazy (Lent), Bridge (Punte) şi Repeater (Repetare).

Lazy (Lent): În acest mod, dispozitivul conectat poate fi în modul Bridge sau Repeater şi poate intra BSSID-ul router-ului pentru a stabili conexiunea.

Bridge (Punte): Puteți conecta wireless două sau mai multe rețele prin cablu prin intermediul acestui mod. În acest mod, trebuie să adăugați adresa wireless MAC a dispozitivului de conectare în tabelul adresei AP MAC a router-ului sau să selectați una din tabelul de scanare.

Repeater Mode (Mod Repetare): În acest mod, adăugați adresa MAC opusă în fiecare tabel al adresei AP MAC manual sau prin intermediul scanner-ului pentru a mări şi extinde proporția wireless.

Capitolul 7: Server DHCP

7.1 Setări DHCP

DHCP (Dynamic Host Control Protocol – Protocolul de Control Host Dinamic) repartizează o adresă IP computerelor din rețeaua LAN / privată. Atunci când activați Serverul DHCP, Serverul DHCP va aloca automat o adresă IP neutilizată din gama adreselor IP către computerul care o cere, în vederea activării „Obtain an IP Address Automatically” (Obținerea Automată a unei Adrese IP). Astfel, este necesară specificarea începerii şi finalizării adresei din gama Adreselor.

- **DHCP Server (Server DHCP)**: Activați checkbox pentru a activa serverul DHCP.
- **IP Address Start/End (Inițiere / Terminare Adresă IP)**: Introduceți gama adresei IP pentru distribuția serverului DHCP.
- **Lease Time (Timp de acordare)**: Durata perioadei de acordare adresă IP.

Capitolul 8: Upgradare Firmware

8.1 Router-ul asigură upgradarea firmware-ului prin click pe „Upgrade” (Upgradare) după căutarea pachetului de upgradare firmware pe care îl puteți descărca de pe www.nedis.nl

- **Browse (Căutare)**: Faceți click pe acest buton pentru selectarea fişierului de upgradare.
- **Upgrade (Upgradare)**: Faceți click pe acest buton pentru a începe procesul de upgradare. După ce upgradarea este finalizată, Router-ul se va reboot-a automat.

8.2 Reboot-area Router-ului

Reboot-area Router-ului face ca setările configurate să intre în vigoare sau instalează Router-ul din nou, dacă setările au eşuat.

8.3 Modificarea parolei

Această secțiune este destinată setării unui nou nume de utilizator şi unei noi parole pentru a vă securiza mai bine router-ul şi rețeaua.

- **User Name (Nume de utilizator)**: Introduceți un nou nume de utilizator pentru dispozitiv.
- **Old Password (Parola veche)**: Introduceți parola veche.
- **New Password (Parola nouă)**: Introduceți o parolă nouă.
- **Re-enter to Confirm (Reintroduceți parola pentru confirmare)**: Reintroduceți parola nouă pentru a o confirma.

8.4 Delogare

După ce ați terminat setările în totalitate, click pe „Yes” (Da) din pagina de delogare pentru a vă deloga de la pagina de gestionare web.

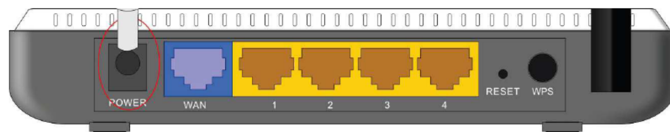
Modul de instalare şi configurare a unui ruter cu un modem prin cablu sau ADSL

Atenție!

Urmați aceşti paşi fără a omite niciunul

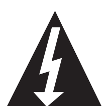
1. Opriți modemul (deconectați-l de la alimentarea electrică principală).
2. Opriți PC-ul/laptopul.
3. Conectați **ieşirea LAN** a modemului prin **cablul LAN** la **portul albastru** al ruterului.

4. Conectați unul dintre **porturile galbene** prin **cablul LAN** la PC/laptop.



5. Acum, porniți modemul şi aşteptați să se conecteze complet (această fază poate dura puțin).
6. Porniți ruterul şi aşteptați cel puțin 30 de secunde.
7. Porniți PC-ul/laptopul şi aşteptați să intre complet în sistem.
8. Deschideți browserul şi navigați la adresa http://192.168.0.1.
9. Introduceți-vă numele şi parola (ambele sunt implicit: **admin**).
10. Navigați la **Setup Wizzard (Asistent de configurare)** şi faceți clic pe **Auto Detect (Autodetectare)**.
11. Acum, faceți clic pe **Next (Următorul),** iar în următorul ecran, pe **Apply (Aplicare)**.
12. Navigați la meniul **WLAN settings (Setări WLAN)** şi asigurați-vă că **Enable Wireless (Activare wireless)** este bifat.
13. Aici puteți configura denumirea rețelei (SSID) şi canalul.
14. Navigați la submeniul **Security Settings (Setări de securitate)** şi selectați tipul de securitate. Vă recomandăm să selectați întotdeauna **Mixed WPA/WPA2 – Personal (WPA/WPA2 mixt - personal)**.
15. Selectați **WPA Algorithms (Algoritmi WPA)** ca **TKIP&AES**.
16. Schimbați parola din câmpul **Pass Phrase**. Vă recomandăm să selectați o parolă solidă, care să fie alcătuită din litere, numere şi chiar şi 1 sau mai multe caractere speciale.
17. Clic pe **Apply (Aplicare)** pentru a stoca datele.
18. Ieşiți din ecranul browserului; setările dvs. pentru rețeaua wireless şi de securitate au fost realizate. Ca alternativă, puteți deconecta cablul dintre ruter şi PC/laptop pentru a realiza o conexiune wireless (dacă PC-ul/laptopului este prevăzut cu un receptor wireless).

Măsuri de siguranță:



ATENŢIE!
PERICOL DE ELECTROCUTARE
NU-L DESCHIDEȚI!



Pentru a se reduce pericolul de electrocutare, acest produs va fi desfăcut NUMAI de către un tehnician avizat, când este necesară depanarea. Deconectați produsul de la priza de rețea sau alte echipamente în cazul apariției unei probleme. Nu expuneți produsul apei sau umezelii.

Întreținere:

Curățarea trebuie făcută cu o cârpă uscată. Nu folosiți solvenți sau agenți de curățare abrazivi.

Garanție:

Nu oferim nicio garanție şi nu ne asumăm niciun fel de responsabilitate în cazul schimbărilor sau modificărilor aduse acestui produs sau în cazul deteriorării cauzate de utilizarea incorectă a produsului.

Generalități:

- Designul şi specificațiile produsului pot fi modificate fără o notificare prealabilă.
- Toate siglele mărcilor şi denumirile produselor sunt mărci comerciale sau mărci comerciale înregistrate ale proprietarilor de drept şi prin prezenta sunt recunoscute ca atare.
- Acest manual a fost conceput cu atenție. Cu toate acestea, nu se pot oferi drepturi pe baza sa. König Electronic nu acceptă răspunderea pentru nicio eroare din acest manual sau consecințele ce decurg din acestea.
- Păstrați acest manual şi ambalajul pentru consultări ulterioare.

Atenție:



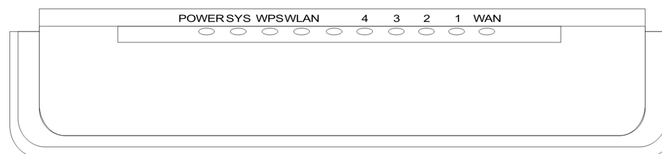
Pe acest produs se află acest marcaj. Acesta semnifică faptul că produsele electrice şi electronice nu trebuie eliminate odată cu gunoiul menajer. Aceste produse au un sistem separat de colectare.

ΕΛΛΗΝΙΚΑ

Κεφάλαιο 1: Εισαγωγή

1.1 Περιγραφή ενδεικτικών λυχνιών LED και θυρών

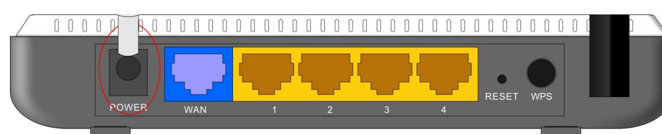
Εικόνα μπροστινής πλευράς του πίνακα και ενδεικτικών λυχνιών LED



Περιγραφή των ενδεικτικών λυχνιών LED στη μπροστινή πλευρά του πίνακα (από αριστερά προς τα δεξιά):

- **POWER**
  Όταν η πράσινη λυχνία ανάβει σταθερά, υποδεικνύει ότι το προϊόν τροφοδοτείται κανονικά.
- **SYS**
  Όταν η πράσινη λυχνία αναβοσβήνει, υποδεικνύει ότι το σύστημα λειτουργεί κανονικά.
- **WPS**
  Όταν αναβοσβήνει, υποδεικνύει ότι η συσκευή επικοινωνεί με τον πελάτη σε λειτουργία WPS.
- **WLAN**
  Ενδεικτική λυχνία LED ασύρματου σήματος. Όταν η πράσινη λυχνία αναβοσβήνει, υποδεικνύει ότι έχει ενεργοποιηθεί η ασύρματη λειτουργία.
- **LAN (4, 3, 2, 1)**
  Ενδεικτική λυχνία LED ενσύρματου τοπικού δικτύου. Όταν ανάβει σταθερά, υποδεικνύει ότι έχει γίνει σύνδεση με τη συσκευή Ethernet. Όταν αναβοσβήνει, υποδεικνύει ότι η συσκευή μεταδίδει ή/και λαμβάνει δεδομένα.
- **WAN**
  Ενδεικτική λυχνία κατάστασης σύνδεσης δικτύου WAN. Όταν παραμένει αναμμένη, υποδεικνύει την κατάσταση σύνδεσης δικτύου του router.

Εικόνα πίσω πλευράς του πίνακα:



Πίσω πλευρά του router **(από αριστερά προς τα δεξιά):**

- **POWER**

Πρόκειται για την υποδοχή σύνδεσης του τροφοδοτικού. Χρησιμοποιήστε το συνοδευτικό τροφοδοτικό ρεύματος 9V DC.

- **WAN**

Θύρα Ethernet 100Mbps με δυνατότητα σύνδεσης σε MODEM, μεταγωγείς switch, router και άλλες συσκευές Ethernet για σύνδεση στο διαδίκτυο μέσω MODEM DSL, ενσύρματου MODEM και ISP.

- **LAN (1, 2, 3, 4)**

4 θύρες Ethernet 10/100Mbps με δυνατότητα σύνδεσης σε μεταγωγείς Ethernet, router Ethernet και κάρτες NIC.

- **RESET**

Πλήκτρο επαναφοράς του συστήματος. Πιέζοντας αυτό το πλήκτρο για 7 δευτερόλεπτα, διαγράφονται οι αποθηκευμένες ρυθμίσεις της συσκευής και γίνεται επαναφορά των προεπιλεγμένων ρυθμίσεων.

- **WPS**

Πιέζοντας αυτό το πλήκτρο για 1 δευτερόλεπτο, ενεργοποιείται το χαρακτηριστικό WPS και αναβοσβήνει η ενδεικτική λυχνία WPS.

Κεφάλαιο 2: Εγκατάσταση υλικού

2.1 Τρόπος εγκατάστασης του router

Χρησιμοποιήστε τον συνοδευτικό τροφοδοτικό για την τροφοδοσία του router. ΣΗΜΑΝΤΙΚΟ: Η χρήση διαφορετικού τροφοδοτικού μπορεί να προκαλέσει βλάβες και να ακυρώσει την εγγύηση αυτού του προϊόντος. Συνδέστε τη θύρα LAN του router με τον προσαρμογέα δικτύου του υπολογιστή σας μέσω καλωδίου. Συνδέστε τη γραμμή ευρυζωνικής πρόσβασης του ISP σας στη θύρα WAN. Εισάγετε το συνοδευτικό CD-ROM στη μονάδα CD-ROM, κάντε διπλό κλικ στο εικονίδιο «Setup» (Εγκατάσταση) και ακολουθήστε τις οδηγίες για να ολοκληρώσετε την εγκατάσταση. Μπορείτε να ρυθμίσετε τις παραμέτρους και από την τοποθεσία web του router. (Για περισσότερες πληροφορίες ανατρέξτε στο Κεφάλαιο 3.)

Κεφάλαιο 3: Τρόπος σύνδεσης στο router

3.1 Τρόπος ρύθμισης των παραμέτρων δικτύου

1. Από την επιφάνεια εργασίας του υπολογιστή σας κάντε δεξί κλικ στην επιλογή «My Network Places» (Θέσεις δικτύου) και επιλέξτε «Properties» (Ιδιότητες).
2. Κάντε δεξί κλικ στην επιλογή «Local Area Network Connection» (Σύνδεση τοπικού δικτύου) και επιλέξτε «Properties» (Ιδιότητες).
3. Επιλέξτε «Internet Protocol (TCP/IP)» [Πρωτόκολλο Internet (TCP/IP)] και κάντε κλικ στην επιλογή «Properties» (Ιδιότητες).
4. - Επιλέξτε «Obtain an IP address automatically» (Αυτόματη απόδοση διεύθυνσης IP) και «Obtain DNS server address automatically» (Αυτόματη απόδοση διεύθυνσης διακομιστή DNS). Κάντε κλικ στην επιλογή «OK» για αποθήκευση των παραμέτρων.
   - Ή επιλέξτε «Use the following IP address» (Χρήση της παρακάτω διεύθυνσης IP) και εισάγετε διεύθυνση IP, μάσκα υποδικτύου και προεπιλεγμένη πύλη ως εξής: Διεύθυνση IP: 192.168.0.XXX: (το XXX αντιστοιχεί σε αριθμό από 2~254), Μάσκα υποδικτύου: 255.255.255.0.
   Πύλη: 192.168.0.1. Θα πρέπει οπωσδήποτε να εισάγετε τη διεύθυνση διακομιστή DNS που σας χορηγήθηκε από τον ISP σας. Διαφορετικά μπορείτε να χρησιμοποιήσετε την προεπιλεγμένη πύλη του router ως διακομιστή μεσολάβησης DNS. Κάντε κλικ στην επιλογή «OK» για αποθήκευση των παραμέτρων.

3.2 Σύνδεση στο router

1. Για να εισέλθετε στη διασύνδεση web του router, ανοίξτε ένα πρόγραμμα περιήγησης διαδικτύου, όπως π.χ. το Internet Explorer ή το Firefox, και εισάγετε την προεπιλεγμένη διεύθυνση IP του router, http://192.168.0.1. Πιέστε «Enter».
2. Πληκτρολογήστε τον κωδικό «admin» στα πεδία Όνομα χρήστη και Κωδικός πρόσβασης. Κάντε κλικ στην επιλογή «OK».

Προεπιλεγμένες ρυθμίσεις	
Διεύθυνση IP	192.168.0.1
Κωδικός πρόσβασης	admin
SSID	KONIG
Λειτουργία ασφαλείας	Απενεργοποιημένο
Ασύρματη λειτουργία	Μεικτή λειτουργία b/g/n
Κανάλι	Αυτόματη επιλογή
Ζώνη ώρας	

Ρυθμίσεις WPS	Ενεργοποιημένες
Όνομα συσκευής UPNP	Ασύρματος router ευρείας ζώνης 11N
Κατασκευαστής UPNP	KONIGELECTRONIC
Όνομα μοντέλου UPNP	CMP-WNROUT41
Αριθμός μοντέλου UPNP	V 1.0
Θεωρητική ταχύτητα δικτύου UPNP	300Mbps
Διεύθυνση συσκευής UPNP	http://192.168.0.1
UPNP	Απενεργοποιημένο

Κεφάλαιο 4: Σύντομος οδηγός εγκατάστασης

4.1 Οδηγός εγκατάστασης

Καλωσορίσατε στον οδηγό εγκατάστασης για τη γρήγορη ρύθμιση των παραμέτρων του router σας. Κάντε κλικ στην επιλογή «Next» (Επόμενο).

Από αυτή την οθόνη, επιλέξτε το είδος της σύνδεσής σας στο διαδίκτυο. Αν δεν είστε βέβαιοι, πιέστε το πλήκτρο «Detect» (Ανίχευση) ή επικοινωνήστε με τον πάροχο υπηρεσιών διαδικτύου, και κάντε κλικ στην επιλογή «Next» (Επόμενο).

Εικονική κλήση ADSL (μέσω PPPoE)

Εισάγετε τον αριθμό λογαριασμού και τον κωδικό πρόσβασης που λάβατε από τον ISP σας, και κάντε κλικ στην επιλογή «Next» (Επόμενο).

Δυναμική διεύθυνση IP (μέσω DHCP)

Αν η σύνδεσή σας έχει δυναμική διεύθυνση IP, σημαίνει ότι η διεύθυνση IP αλλάζει κάθε φορά που συνδέεστε. Δεν χρειάζεται να γίνει εισαγωγή των πληροφοριών όπως στις υπόλοιπες λειτουργίες. Κάντε κλικ στις επιλογές «Next» (Επόμενο) και «Save» (Αποθήκευση) για ολοκλήρωση της ρύθμισης.

Στατική διεύθυνση IP

Από αυτή την οθόνη, εισάγετε τις πληροφορίες διεύθυνσης δικτύου που λάβατε από τον ISP σας στα πεδία Διεύθυνση IP, Μάσκα υποδικτύου, Πύλη και Κύριος διακομιστής DNS, και κάντε κλικ στην επιλογή «Next» (Επόμενο).

L2TP

Ζητήστε τις απαιτούμενες πληροφορίες από τον ISP σας.

Κεφάλαιο 5: Ρυθμίσεις για προχωρημένους

5.1 Ρυθμίσεις LAN

Οι ρυθμίσεις LAN αποτελούν τις βασικές παραμέτρους TCP/IP των θυρών LAN.

- **Διεύθυνση IP**: Οι διευθύνσεις IP του LAN του router (όχι η διεύθυνση IP του υπολογιστή σας). Η προεπιλεγμένη τιμή είναι 192.168.0.1.
- **Μάσκα υποδικτύου**: Δείχνει τη μάσκα υποδικτύου του router για υπολογισμό του μεγέθους του δικτύου. Η προεπιλεγμένη τιμή είναι 255.255.255.0.

ΣΗΜΑΝΤΙΚΟ:

Αν αλλάξετε τη διεύθυνση IP, θα πρέπει να τη θυμάστε την επόμενη φορά που θα επιχειρήσετε να συνδεθείτε στο βοηθητικό πρόγραμμα web.

5.2 Ρυθμίσεις WAN

Αφού επιλέξετε τον τύπο σύνδεσης ISP από τον Οδηγό Εγκατάστασης, μπορείτε -εφόσον επιθυμείτε να τροποποιήσετε τις σχετικές ρυθμίσεις- να προβείτε σε λεπτομερή τροποποίηση και παραμετροποίηση των ρυθμίσεων από εδώ.

Στατική διεύθυνση IP

Αν έχετε επιλέξει λειτουργία σύνδεσης με στατική διεύθυνση IP, μπορείτε να τροποποιήσετε τις ακόλουθες πληροφορίες διεύθυνσης.

- **Διεύθυνση IP**: Εισάγετε τη διεύθυνση WAN IP που λάβατε από τον ISP σας εδώ.
- **Μάσκα υποδικτύου**: Εισάγετε τη μάσκα υποδικτύου WAN εδώ.
- **Πύλη**: Εισάγετε την πύλη WAN εδώ.
- **Κύριος διακομιστής DNS**: Εισάγετε τον κύριο διακομιστή DNS που λάβατε από τον ISP σας.
- **Δευτερεύων διακομιστής DNS**: Εισάγετε το δευτερεύοντα διακομιστή DNS.

Κεφάλαιο 6: Ρύθμιση ασύρματης σύνδεσης

6.1 Βασικές ρυθμίσεις

- **Ενεργοποίηση ασύρματης σύνδεσης**: Μαρκάρετε για ενεργοποίηση των ασύρματων χαρακτηριστικών του router. Ξεμαρκάρετε για απενεργοποίηση.
- **Λειτουργία δικτύου**: Επιλέξτε μία από τις ακόλουθες λειτουργίες. Η προεπιλεγμένη λειτουργία είναι 11b/g/n.
- **Κύριο SSID**: Το SSID (Service Set Identifier / Αναγνωριστικό Συνόλου Υπηρεσιών) είναι το μοναδικό όνομα του ασύρματου δικτύου. Η συσκευή διαθέτει δύο SSID, ενώ το κύριο SSID είναι απαραίτητο.
- **Δευτερεύον SSID**: Αυτό είναι προαιρετικό.
- **Μετάδοση (SSID)**: Επιλέξτε «Enable» (Ενεργοποίηση) για ενεργοποίηση του SSID της συσκευής, ώστε να είναι ορατό στους ασύρματους πελάτες. Η προεπιλεγμένη ρύθμιση είναι «ενεργό».
- **Απομόνωση σημείου πρόσβασης MBSSID**: Χαρακτηριστικό ελέγχου πρόσβασης που βασίζεται σε ασύρματη διεύθυνση MAC. Όταν το χαρακτηριστικό είναι ενεργοποιημένο, οι ασύρματοι πελάτες που συνδέονται στο ίδιο SSID δεν μπορούν να επικοινωνήσουν μεταξύ τους.
- **Απομόνωση σημείου πρόσβασης**: Χαρακτηριστικό ελέγχου πρόσβασης που βασίζεται στο SSID. Όταν το χαρακτηριστικό είναι ενεργοποιημένο, οι ασύρματοι πελάτες διαθέτουν ξεχωριστά εικονικά δίκτυα και δεν μπορούν να επικοινωνήσουν μεταξύ τους. Όταν το χαρακτηριστικό είναι ενεργοποιημένο, οι ασύρματοι πελάτες που συνδέονται με το κύριο SSID και το δευτερεύον SSID δεν μπορούν να επικοινωήσουν μεταξύ τους, γεγονός που προσφέρει μεγάλη ασφάλεια στο ασύρματο δίκτυο.
- **Κανάλι**: Ορίστε το ενεργό κανάλι (από 1 έως 13\Auto) του ασύρματου δικτύου.
- **Κανάλι επέκτασης**: Για να αυξήσετε την ταχύτητα μετάδοσης δεδομένων του ασύρματου δικτύου, το εύρος του καναλιού επέκτασης ορίζεται σε λειτουργία 11n.
- **Εύρος ζώνης καναλιού**: Επιλέξτε το εύρος ζώνης καναλιού για να βελτιώσετε την ασύρματη απόδοση. Όταν στο δίκτυο υπάρχουν πελάτες 11b/g και 11n, μπορείτε να επιλέξετε 40M. Όταν πρόκειται για δίκτυο 11n, επιλέξτε 20/40M για βελτίωση της μετάδοσης δεδομένων.

6.2 Ασύρματες ρυθμίσεις ασφαλείας

Από εδώ μπορείτε να ρυθμίσετε τις παραμέτρους ασφαλείας του σημείου πρόσβασης (AP) του δικτύου. Παρουσιάζουμε έξι (από τις δέκα) κοινές μεθόδους κρυπτογράφησης, συμπεριλαμβανομένων των Mixed WEP (Μικτό WEP), WPA-personal (WPA-προσωπικό), WPA-enterprise (WPA-επιχείρησης), WPA2-personal (WPA2-προσωπικό), WPA2- enterprise (WPA2-επιχείρησης), κτλ.

6.2.1 Mixed WEP

Το WEP (Wired Equivalent Privacy / Εμπιστευτικότητα αντίστοιχη με ενσύρματο δίκτυο) είναι μια βασική μέθοδος κρυπτογράφησης, η οποία χρησιμοποιείται συνήθως για την κρυπτογράφηση ασύρματων δεδομένων μέσω μιας σειράς ψηφιακών κλειδιών (μήκους 64 bits ή 128 bits). Χρησιμοποιώντας τα ίδια κλειδιά σε όλες τις συσκευές του ασύρματου δικτύου, μπορείτε να αποτρέψετε την παρακολούθηση των μεταδόσεών σας και τη χρήση των ασύρματων πόρων σας από μη εξουσιοδοτημένες ασύρματες συσκευές. Επιλέξτε τη μέθοδο Mixed WEP για να μεταβείτε στο ακόλουθο παράθυρο:

- **Επιλογή SSID**: Επιλέξτε SSID (κύριο SSID ή δευτερεύον SSID) για να ρυθμίσετε τις παραμέτρους ασφαλείας από το κυλιόμενο μενού.
- **Λειτουργία ασφαλείας**: Από το κυλιόμενο μενού, επιλέξτε τις αντίστοιχες λειτουργίες κρυπτογράφησης ασφαλείας.
- **Κλειδιά WEP 1~4**: Ρυθμίστε το κλειδί WEP σε μορφή ASCII και Hex. Μπορείτε να εισάγετε κωδικό ASCII (5 ή 13 χαρακτήρες ASCII, δεν επιτρέπεται η χρήση μη έγκυρων χαρακτήρων, όπως το «/») ή 10/26 χαρακτήρες hex.
- **Προεπιλεγμένο κλειδί**: Επιλέξτε ένα από τα τέσσερα παραμετροποιημένα κλειδιά ως τρέχον κλειδί.

6.2.2 WPA-Personal

Το WPA (Wi-Fi Protected Access / Προστατευμένη πρόσβαση Wi-Fi) είναι ένα πρότυπο Wi-Fi, το οποίο αποτελεί ένα νεότερο σχέδιο ασύρματης κρυπτογράφησης που σχεδιάστηκε για τη βελτίωση των χαρακτηριστικών ασφαλείας του WEP. Χρησιμοποιεί πιο ισχυρούς τύπους κρυπτογράφησης [όπως το TKIP (Temporal Key Integrity Protocol / Πρωτόκολλο ακεραιότητας προσωρινού κλειδιού) και το AES (Advanced Encryption Standard / Προηγμένο πρότυπο κρυπτογράφησης)] και μπορεί να αλλάζει τα κλειδιά με δυναμικό τρόπο για κάθε εξουσιοδοτημένη ασύρματη συσκευή.

- **Επιλογή SSID**: Επιλέξτε SSID (κύριο SSID ή δευτερεύον SSID) για να ρυθμίσετε τις παραμέτρους ασφαλείας από το κυλιόμενο μενού.
- **Αλγόριθμοι WPA**: Προσφέρει TKIP (Temporal Key Integrity Protocol) ή AES (Advanced Encryption Standard). Η προεπιλεγμένη λειτουργία είναι TKIP.
- **Φράση πρόσβασης**: Εισάγετε τους κρυπτογραφημένους χαρακτήρες με 8-63 χαρακτήρες ASCII.
- **Διάστημα ανανέωσης κλειδιού**: Ορίστε την περίοδο ανανέωσης του κλειδιού.

6.2.3 WPA2- Personal

Το WPA2 (Wi-Fi Protected Access version 2 / Προστατευμένη πρόσβαση Wi-Fi, έκδοση 2) προσφέρει υψηλότερη ασφάλεια σε σύγκριση με το WEP (Wireless Equivalent Privacy) και το WPA (Wi-Fi Protected Access).

- **Επιλογή SSID**: Επιλέξτε SSID (κύριο SSID ή δευτερεύον SSID) για να ρυθμίσετε τις παραμέτρους ασφαλείας από το κυλιόμενο μενού.
- **Αλγόριθμοι WPA**: Προσφέρει TKIP (Temporal Key Integrity Protocol) ή AES (Advanced Encryption Standard). Η προεπιλεγμένη λειτουργία είναι TKIP.
- **Φράση πρόσβασης**: Εισάγετε τους κρυπτογραφημένους χαρακτήρες με 8-63 χαρακτήρες ASCII.
- **Διάστημα ανανέωσης κλειδιού**: Ορίστε την περίοδο ανανέωσης του κλειδιού.

6.2.4 WPA- Enterprise

Αυτή η λειτουργία ασφαλείας χρησιμοποιείται όταν η συσκευή συνδέεται με κάποιον διακομιστή RADIUS. Επιλέξτε «WPA-Enterprise» από το κυλιόμενο μενού για να μεταβείτε στο ακόλουθο παράθυρο:

- **Επιλογή SSID**: Επιλέξτε SSID (κύριο SSID ή δευτερεύον SSID) για να ρυθμίσετε τις παραμέτρους ασφαλείας από το κυλιόμενο μενού.
- **Αλγόριθμοι WPA**: Προσφέρει TKIP (Temporal Key Integrity Protocol) ή AES (Advanced Encryption Standard). Η προεπιλεγμένη λειτουργία είναι TKIP.
- **Διάστημα ανανέωσης κλειδιού:** Ορίστε την περίοδο ανανέωσης του κλειδιού.
- **Διακομιστής Radius**: Εισάγετε τη διεύθυνση IP του διακομιστή Radius.
- **Θύρα διακομιστή Radius**: Εισάγετε τη θύρα ελέγχου ταυτότητας του διακομιστή Radius. Η προεπιλεγμένη ρύθμιση είναι 1812.
- **Κοινόχρηστος μυστικός κωδικός**: Εισάγετε το κοινόχρηστο κλειδί για το διακομιστή ελέγχου ταυτοτήτων με 8~63 χαρακτήρες ASCII.
- **Χρονικό όριο περιόδου λειτουργίας**: Το διάστημα ελέγχου ταυτότητας μεταξύ του AP και του διακομιστή ελέγχου ταυτοτήτων.

6.2.5 WPA2-Enterprise

Αυτή η λειτουργία ασφαλείας βασίζεται σε διακομιστή ελέγχου ταυτοτήτων Radius και τη μέθοδο κρυπτογράφησης WPA2. Το WPA2 χρησιμοποιείται όταν η συσκευή συνδέεται με κάποιον διακομιστή RADIUS. Επιλέξτε «WPA2-Enterprise» από το κυλιόμενο μενού για να μεταβείτε στο ακόλουθο παράθυρο:

- **Επιλογή SSID**: Επιλέξτε SSID (κύριο SSID ή δευτερεύον SSID) για να ρυθμίσετε τις παραμέτρους ασφαλείας από το κυλιόμενο μενού.
- **Αλγόριθμοι WPA**: Προσφέρει TKIP (Temporal Key Integrity Protocol) ή AES (Advanced Encryption Standard). Η προεπιλεγμένη λειτουργία είναι TKIP.
- **Διάστημα ανανέωσης κλειδιού**: Ορίστε την περίοδο ανανέωσης του κλειδιού.
- **Διακομιστής Radius**: Εισάγετε τη διεύθυνση IP του διακομιστή Radius.
- **Θύρα διακομιστή Radius**: Εισάγετε τη θύρα ελέγχου ταυτότητας του διακομιστή Radius. Η προεπιλεγμένη ρύθμιση είναι 1812.
- **Κοινόχρηστος μυστικός κωδικός**: Εισάγετε το κοινόχρηστο κλειδί για το διακομιστή ελέγχου ταυτοτήτων με 8~63 χαρακτήρες ASCII.
- **Χρονικό όριο περιόδου λειτουργίας**: Το διάστημα ελέγχου ταυτότητας μεταξύ του AP και του διακομιστή ελέγχου ταυτοτήτων. Η προεπιλεγμένη ρύθμιση είναι 3600 δευτερόλεπτα.

6.2.6 802.1X

Αυτή η λειτουργία ασφαλείας χρησιμοποιείται όταν η συσκευή συνδέεται με κάποιον διακομιστή RADIUS. Το 802.1x είναι ένα είδος πρωτοκόλλου ελέγχου ταυτότητας που βασίζεται σε θύρα, το οποίο συνδυάζει έναν τύπο ελέγχου ταυτότητας και μια στρατηγική από πλευράς των χρηστών. Η θύρα μπορεί να είναι φυσική ή λογική (όπως το VLAN). Αν χρησιμοποιείτε ασύρματο LAN, η θύρα είναι απλώς ένα κανάλι. Στόχος του ελέγχου ταυτότητας 802.11x είναι να διαπιστωθεί αν είναι δυνατή η χρήση της θύρας. Αν ο έλεγχος ταυτότητας της θύρας ολοκληρωθεί με επιτυχία, μπορείτε να ανοίξετε τη θύρα, επιτρέποντας τη διακίνηση όλων των μηνυμάτων. Αν ο έλεγχος ταυτότητας της θύρας δεν ολοκληρωθεί με επιτυχία, μπορείτε να αφήσετε τη θύρα απενεργοποιημένη, επιτρέποντας μόνο τη διακίνηση μηνυμάτων με πρωτόκολλο ελέγχου ταυτότητας 802.1x. Επιλέξτε «802.1x» από το κυλιόμενο μενού για να μεταβείτε στο ακόλουθο παράθυρο:

- **Επιλογή SSID**: Επιλέξτε SSID (κύριο SSID ή δευτερεύον SSID) για να ρυθμίσετε τις παραμέτρους ασφαλείας από το κυλιόμενο μενού.
- **WEP**: Κάντε κλικ στην επιλογή «Enable/Disable» (Ενεργοποίηση/Απενεργοποίηση) για να ενεργοποιήσετε ή να απενεργοποιήσετε τον αλγόριθμο WEP.
- **Διακομιστής Radius**: Εισάγετε τη διεύθυνση IP του διακομιστή Radius.
- **Θύρα διακομιστή Radius**: Εισάγετε τη θύρα ελέγχου ταυτότητας του διακομιστή Radius. Η προεπιλεγμένη ρύθμιση είναι 1812.
- **Κοινόχρηστος μυστικός κωδικός**: Εισάγετε το κοινόχρηστο κλειδί για το διακομιστή ελέγχου ταυτοτήτων με 8~63 χαρακτήρες ASCII.
- **Χρονικό όριο περιόδου λειτουργίας:** Το διάστημα ελέγχου ταυτότητας μεταξύ του AP και του διακομιστή ελέγχου ταυτοτήτων. Η προεπιλεγμένη ρύθμιση είναι 3600 δευτερόλεπτα.

6.4 Ρυθμίσεις WPS

Το WPS (Wi-Fi Protected Setting / Προστατευμένη ρύθμιση Wi-Fi) μπορεί να χρησιμοποιηθεί για την εύκολη και γρήγορη εγκατάσταση της σύνδεσης μεταξύ των πελατών του ασύρματου δικτύου και της συσκευής μέσω κρυπτογραφημένων περιεχομένων. Το μόνο που πρέπει να κάνει ο χρήστης είναι να εισάγει έναν κωδικό PIN ή να πιέσει το πλήκτρο WPS του πίνακα για να ρυθμίσει τις παραμέτρους αυτόματα, χωρίς να χρειάζεται χειροκίνητη επιλογή μεθόδου κρυπτογράφησης και μυστικών κλειδιών. Από το μενού «Wireless settings» (Ρυθμίσεις ασύρματης σύνδεσης), κάντε κλικ στην επιλογή «WPS settings» (Ρυθμίσεις WPS) για να μεταβείτε στην επόμενη οθόνη.

- **Ρυθμίσεις WPS**: Για ενεργοποίηση ή απενεργοποίηση της λειτουργίας WPS. Η προεπιλεγμένη ρύθμιση είναι «ανενεργό».
- **Λειτουργία WPS**: Προσφέρονται δύο επιλογές: PBC (Push-Button Configuration / Ρύθμιση παραμέτρων με το πάτημα ενός κουμπιού) και κωδικός PIN.
- **PBC**: Επιλέξτε PBC ή πιέστε το πλήκτρο WPS στη μπροστινή πλευρά του πίνακα της συσκευής για περίπου ένα δευτερόλεπτο. (Πιέζοντας το πλήκτρο για ένα περίπου δευτερόλεπτο, η ένδειξη WPS αναβοσβήνει για 2 λεπτά, υποδεικνύοντας ότι το WPS έχει ενεργοποιηθεί. Όσο η λυχνία αναβοσβήνει, μπορείτε να ενεργοποιήσετε κάποια άλλη συσκευή, δημιουργώντας μεταξύ τους επικοινωνία WPS/PBC. Η ένδειξη WPS σβήνει μετά από δύο λεπτά, υποδεικνύοντας ότι η σύνδεση WPS έχει ολοκληρωθεί. Σε περίπτωση προσθήκης περισσότερων πελατών, επαναλάβετε τα παραπάνω βήματα. Προς το παρόν το WPS υποστηρίζει την πρόσβαση έως και 32 πελατών.)
- PIN: Όταν είναι ενεργοποιημένη αυτή η επιλογή, θα πρέπει να πληκτρολογήσετε στο πεδίο τον κωδικό PIN του ασύρματου πελάτη και να διατηρήσετε τον ίδιο κωδικό στον πελάτη WPS.

6.5 Ρυθμίσεις WDS

Το WDS (Wireless Distribution System / Σύστημα ασύρματης διανομής) χρησιμοποιείται για την επέκταση του πεδίου ασύρματης κάλυψης. Αυτό το router προσφέρει τρεις λειτουργίες: Lazy (Αργή), Bridge (Γέφυρα) και Repeater (Επαναλήπτης).

Lazy: Σε αυτή τη λειτουργία, η συνδεμένη συσκευή θα πρέπει να βρίσκεται σε λειτουργία Bridge ή Repeater. Εισάγετε το BSSID για να εγκαταστήσετε τη σύνδεση.

Bridge: Μέσω αυτής της λειτουργίας μπορείτε να συνδέσετε ασύρματα δύο ή περισσότερα ενσύρματα δίκτυα. Σε αυτή τη λειτουργία θα πρέπει να προσθέσετε την ασύρματη διεύθυνση MAC της συσκευής σύνδεσης στον πίνακα διευθύνσεων MAC του AP του router ή να επιλέξετε μια διεύθυνση από τη σάρωση πίνακα.

Λειτουργία Repeater: Σε αυτή τη λειτουργία, προσθέστε την αντίθετη διεύθυνση MAC στον πίνακα διευθύνσεων MAC των AP χειροκίνητα ή μέσω σάρωσης για να διευρύνετε και να επεκτείνετε την ακτίνα ασύρματης εκπομπής.

Κεφάλαιο 7: Διακομιστής DHCP

7.1 Ρυθμίσεις DHCP

Το DHCP (Dynamic Host Control Protocol / Πρωτόκολλο δυναμικού ελέγχου κεντρικών υπολογιστών) αντιστοιχίζει μια διεύθυνση IP στους υπολογιστές του LAN/ιδιωτικού δικτύου. Κατά την ενεργοποίηση του διακομιστή DHCP, ο διακομιστής DHCP αναθέτει αυτόματα μια μη χρησιμοποιημένη διεύθυνση IP από τη δεξαμενή διευθύνσεων IP στον υπολογιστή που υπέβαλε το αίτημα, εφόσον έχει ενεργοποιηθεί η επιλογή «Obtain an IP Address Automatically» (Αυτόματη απόδοση διεύθυνσης IP). Επομένως, απαιτείται προσδιορισμός τις αρχικής και τελικής διεύθυνσης από τη δεξαμενή διευθύνσεων IP.

- **Διακομιστής DHCP**: Μαρκάρετε το κουτάκι για να ενεργοποιήσετε το διακομιστή DHCP.
- **Αρχική/τελική διεύθυνση IP**: Εισάγετε το εύρος των διευθύνσεων IP για διανομή από το διακομιστή DHCP.
- **Χρόνος εκμίσθωσης**: Η διάρκεια της εκμίσθωσης της διεύθυνσης IP.

Κεφάλαιο 8: Αναβάθμιση υλικολογισμικού

8.1 Το router προσφέρει τη δυνατότητα αναβάθμισης του υλικολογισμικού κάνοντας κλικ στην επιλογή «Upgrade» (Αναβάθμιση) μετά την αναζήτηση στο πακέτο αναβάθμισης υλικολογισμικού, το οποίο μπορείτε να κατεβάσετε από τη διεύθυνση www.nedis.nl

- **Browse (Αναζήτηση)**: πιέστε αυτό το πλήκτρο για να επιλέξετε αρχείο αναβάθμισης.
- **Upgrade (Αναβάθμιση)**: πιέστε αυτό το πλήκτρο για να ξεκινήσετε τη διαδικασία αναβάθμισης. Μετά την ολοκλήρωση της αναβάθμισης, το router προβαίνει αυτόματα σε επανεκκίνηση.

8.2 Επανεκκίνηση router

Κατά την επανεκκίνηση του router τίθενται σε λειτουργία οι νέες ρυθμίσεις ή επαναφέρονται οι προεπιλεγμένες ρυθμίσεις του router σε περίπτωση αποτυχίας.

8.3 Αλλαγή κωδικού πρόσβασης

Σε αυτή την ενότητα παρουσιάζεται ο τρόπος ρύθμισης νέου ονόματος χρήστη και κωδικού πρόσβασης για καλύτερη προστασία του router και του δικτύου.

- **Όνομα χρήστη**: Εισάγετε νέο όνομα χρήστη για τη συσκευή.
- **Παλιός κωδικός πρόσβασης**: Εισάγετε τον παλιό κωδικό πρόσβασης.
- **Νέος κωδικός πρόσβασης**: Εισάγετε νέο κωδικό πρόσβασης.
- **Εκ νέου εισαγωγή και επιβεβαίωση**: Εισάγετε εκ νέου για επιβεβαίωση του νέου κωδικού πρόσβασης.

8.4 Αποσύνδεση

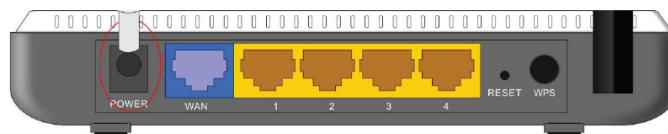
Μετά την ολοκλήρωση της ρύθμισης, κάντε κλικ στην επιλογή «Yes» (Ναι) στη σελίδα αποσύνδεσης για να αποσυνδεθείτε από τη σελίδα διαχείρισης web.

Πώς να εγκαταστήσετε και να ρυθμίσετε ένα ρούτερ σε ένα ενσύρματο ή ADSL μόντεμ

Προσοχή!

Ακολουθήστε όλα τα παρακάτω βήματα με τη σειρά

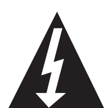
1. Απενεργοποιήστε το μόντεμ (αποσυνδέστε το από το ρεύμα).
2. Απενεργοποιήστε τον υπολογιστή.
3. Συνδέστε την **έξοδο LAN** του μόντεμ στη **μπλε θύρα** του ρούτερ μέσω **καλωδίου LAN**.
4. Συνδέστε τις **κίτρινες θύρες** στον υπολογιστή μέσω **καλωδίου LAN**.



5. Ενεργοποιήστε τώρα το μόντεμ και περιμένετε μέχρι να συνδεθεί κανονικά (μπορεί να διαρκέσει μερικά λεπτά).
6. Ενεργοποιήστε το ρούτερ και περιμένετε τουλάχιστον 30 δευτερόλεπτα.
7. Ενεργοποιήστε τον υπολογιστή και περιμένετε μέχρι να ολοκληρωθεί η φόρτωση του λειτουργικού.
8. Ανοίξτε το πρόγραμμα περιήγησης και μεταβείτε στη διεύθυνση http://192.168.0.1.
9. Εισάγετε όνομα χρήστη και κωδικό πρόσβασης (και τα δύο **admin** από προεπιλογή).
10. Μεταβείτε στο **Setup Wizzard** (Οδηγός εγκατάστασης) και κάντε κλικ στην επιλογή **Auto Detect** (Αυτόματη ανίχνευση).
11. Κάντε τώρα κλικ στην επιλογή **Next** (Επόμενο) και στην επόμενη οθόνη κάντε κλικ στην επιλογή **Apply** (Εφαρμογή).
12. Μεταβείτε στο μενού **WLAN settings** (Ρυθμίσεις WLAN) και βεβαιωθείτε ότι είναι μαρκαρισμένη η επιλογή **Enable Wireless** (Ενεργοποίηση ασύρματου).
13. Από εδώ μπορείτε να ρυθμίσετε το όνομα δικτύου (SSID) και το κανάλι.
14. Μεταβείτε στο υπομενού **Security Settings** (Ρυθμίσεις ασφάλειας) και επιλέξτε τύπο ασφάλειας. Συνιστάται η επιλογή του τύπου **Mixed WPA/WPA2 – Personal** (Μεικτό WPA/WPA2 - Προσωπικό).
15. Επιλέξτε **WPA Algorithms** (Αλγόριθμοι WPA) ως **TKIP&AES**.

16. Αλλάξτε τον κωδικό πρόσβασης στο πεδίο **Pass Phrase** (Φράση πρόσβασης). Συνιστάται η επιλογή ενός δυνατού κωδικού πρόσβασης, αποτελούμενου από γράμματα, αριθμούς και πιθανόν 1 ή περισσότερους ειδικούς χαρακτήρες.
17. Κάντε κλικ στην επιλογή **Apply** (Εφαρμογή) για να αποθηκεύσετε τα δεδομένα.
18. Βγείτε από την οθόνη περιήγησης. Η ρύθμιση του ασύρματου δικτύου και η παραμετροποίηση των ρυθμίσεων ασφάλειας έχει ολοκληρωθεί. Μπορείτε προαιρετικά να αποσυνδέσετε το καλώδιο από το ρούτερ και τον υπολογιστή και να εγκαταστήσετε μια ασύρματη σύνδεση (αν ο υπολογιστής διαθέτει ασύρματο δέκτη).

Οδηγίες ασφαλείας:






Για να μειώσετε τον κίνδυνο ηλεκτροπληξίας, το προϊόν αυτό θα πρέπει να ανοιχθεί ΜΟΝΟ από εξουσιοδοτημένο τεχνικό όταν απαιτείται συντήρηση (σέρβις). Αποσυνδέστε το προϊόν από την πρίζα και άλλο εξοπλισμό αν παρουσιαστεί πρόβλημα. Μην εκθέτετε το προϊόν σε νερό ή υγρασία.

Συντήρηση:
Καθαρίστε μόνο με ένα στεγνό πανί. Μη χρησιμοποιείτε διαλύτες ή λειαντικά.

Εγγύηση:
Ουδεμία εγγύηση ή ευθύνη δεν είναι αποδεκτή σε περίπτωση αλλαγής ή μετατροπής του προϊόντος ή βλάβης που προκλήθηκε λόγω εσφαλμένης χρήσης του προϊόντος.

Γενικά:
- Το σχέδιο και τα χαρακτηριστικά μπορούν να αλλάξουν χωρίς καμία προειδοποίηση.
- Όλα τα λογότυπα, οι επωνυμίες και οι ονομασίες προϊόντων είναι εμπορικά σήματα ή σήματα κατατεθέντα των αντίστοιχων κατόχων και δια του παρόντος αναγνωρίζονται ως τέτοια.
- Αυτό το εγχειρίδιο συντάχτηκε με προσοχή. Ωστόσο, δεν προκύπτουν δικαιώματα. Η König Electronic δεν φέρει καμία ευθύνη για σφάλμα σε αυτό το εγχειρίδιο ή στις συνέπειές τους.
- Φυλάξτε το παρόν εγχειρίδιο και τη συσκευασία για μελλοντική αναφορά.

Προσοχή:



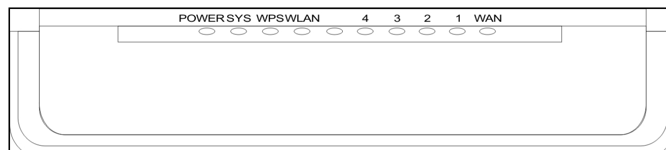
Το συγκεκριμένο προϊόν έχει επισημανθεί με αυτό το σύμβολο. Αυτό σημαίνει ότι οι μεταχειρισμένες ηλεκτρικές και ηλεκτρονικές συσκευές δεν πρέπει να αναμειγνύονται με τα κοινά οικιακά απορρίμματα. Υπάρχει ξεχωριστό σύστημα συλλογής για αυτά τα αντικείμενα.

DANSK

Afsnit 1: Introduktion

1.1 LED-indikator og Port-beskrivelse

Frontpanel og LED-indikatordisplay



Beskrivelse af LED-indikatorlys på frontpanelet: (fra venstre mod højre)

■ **POWER**

Når det grønne lys forbliver tændt, angiver det, at strømforsyningen er i orden.

■ **SYS**

Når det grønne lys blinker, angiver det, at systemet kører korrekt.

■ **WPS**

Når lyset blinker, angiver det, at enheden kommunikerer med klienten i WPS-funktion.

■ **WLAN**

LED-indikator for trådløst signal. Når det grønne lys blinker, angiver det, at trådløs forbindelse er aktiveret.

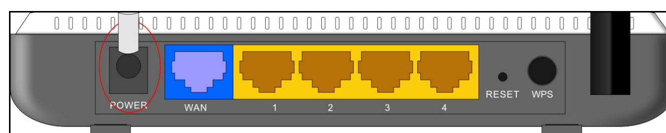
■ **LAN (4, 3, 2, 1)**

LED-indikator for kabelforbindelse til lokalt netværk. Hvis det forbliver tændt, angiver det, at der er forbindelse til Ethernet-enheden; hvis det blinker, angiver det, at enheden er ved at sende og/eller modtage data.

■ **WAN**

Indikator for Wide Area Network. Hvis det forbliver tændt, angiver det routerens W.

Bagpanelets display:



Bagpanel: (fra venstre mod højre)

■ **POWER**

Stikket er for tilslutning af strømforsyningsadapter. Brug venligst den medfølgende 9V DC strømforsyningsadapter.

■ **WAN**

Der kan tilsluttes en 100Mbps Ethernet-port med Modem, Switch, Router og andre Ethernet-enheder til internetforbindelse med DSL-MODEM, Kabelmodem og ISP.

■ **LAN (1, 2, 3, 4)**

4 10/100Mbps Ethernet-porte kan tilsluttes med en Ethernet-kontakt, Ethernet-router og NIC-kort.

■ **RESET**

Nulstillingsknap for systemet. Tryk på denne knap i 7 sekunder, så vil enhedens konfigurerede indstillinger blive slette og fabriksindstillingerne genoprettes.

■ **WPS**

Tryk i 1 sekund, så aktiveres WPS-funktionen og WPS-indikatoren blinker.

Afsnit 2: Hardware-installation

2.1 Sådan installeres routeren

Brug venligst den medfølgende strømforsyningsadapter til routeren. VIGTIGT: Hvis du bruger en anden adapter, kan det forårsage skade og garantien for produktet bortfalder. Tilslut routerens LAN-port til netværksadapteren på din computer med et kabel. Tilslut din bredbåndslinje fra din internetudbyder til WAN-porten. Indsæt den medfølgende CD-ROM i CD-ROM-drevet, dobbeltklik på ”Setup”-ikonet og følg anvisningerne for at fuldføre installationen. Eller du kan gå ind på internetsiden for routeren for at konfigurere den. (Se flere oplysninger i Afsnit 3)

Afsnit 3: Sådan logger du ind til routeren

3.1 Sådan indstilles netværkskonfigurationerne.

1. På din computers skrivebord højreklikker du på ”My Network Places” og vælger ”Properties”.
2. Højreklik på ”Local Area Network Connection” og vælg ”Properties”.
3. Vælg ”Internet Protocol (TCP/IP)” og klik på ”Properties”.
4. - Vælg ”Obtain an IP address automatically” og ”Obtain DNS server address automatically”. Klik på ”OK” for at gemme konfigurationen.
   - Eller vælg ”Use the following IP address” og indtast IP-adresse, Subnet mask og Default gateway på følgende måde: IP-adresse: 192.168.0.XXX: (XXX er et tal fra 2~254) Subnet Mask: 255.255.255.0. Gateway: 192.168.0.1. Du er helt sikkert nødt til at indtaste DNS-serveradressen, som du har fået fra din internetudbyder. I modsat fald kan du bruge routerens standard gateway som DNS proxy server. Klik på ”OK” for at gemme konfigurationen.

3.2 Sådan logger du ind til routeren

1. For at få adgang til routerens internetbaserede brugerflade igangsætter du din internetbrowser som f.eks. Internet Explorer eller Firefox og indtaster routerens standard IP-adresse, http://192.168.0.1. Tryk på ”Enter”.
2. Indtast ”admin” under både brugernavn og password. Klik på OK.

Standardindstilling	
IP-adresse	192.168.0.1
Password	admin
SSID	KONIG
Sikkerhedsfunktion	Deaktiver
Trådløs funktion	b/g/n Mixd Mode
Kanal	Autoselect
Tidszone	
WPS-indstillinger	Aktiver
JPNP enhedsnavn	11N Wireless Broadband Router
JPNP producent	KONIGELECTRONIC
JPNP modelnavn	CMP-WNROUT41
JPNP modelnummer	V 1.0
JPNP nominel netværkshastighed	300Mbps
JPNP enhedsadresse	http://192.168.0.1
UPNP	Deaktiver

Afsnit 4: Hurtig opsætningsguide

4.1 Opsætningsprogram

Her ser du ”Welcome to Setup Wizard” for hurtig konfiguration af din router. Klik på ”Next”.

På denne skærm skal du vælge den type internetforbindelse, som du bruger. Hvis du ikke er sikker, så tryk på ”Detect”-knappen eller kontakt din internetudbyder og klik så på ”Next”.

ADSL Virtual Dial-up (Via PPPoE)

Indtast den konto og adgangskode, som du har fået af din internetudbyder og klik på ”Next”.

Dynamic IP (Via DHCP)

Hvis din forbindelsestype er Dynamic IP, betyder det, at din IP-adresse ændres, hver gang du opretter forbindelse. Du behøver ikke at indtaste oplysningerne under andre funktioner. Klik på ”Next” og herefter på ”Save” for at afslutte indstillingen.

Statisk IP

På denne skærm indtaster du oplysningerne om netværksadressen, som du har fået af din internetudbyder i felterne IP-adresse, Subnet Mask, Gateway og Primary DNS server og klik herefter på ”Next”.

L2TP

Kontakt din internetudbyder for at få de nødvendige oplysninger.

Afsnit 5: Avancerede indstillinger

5.1 LAN-indstillinger

LAN-indstillingerne gælder for de basale TCP/IP-parametre for LAN-portene.

- **IP Address**: Routerens LAN IP-adresser (ikke din PCs IP-adresse). 192.168.0.1 er standardværdien.
- **Subnet Mask**: Viser routerens subnet-maske til måling af netværksstørrelsen. 255.255.255.0 er standardværdien.

VIGTIGT:

Når du har ændret IP-adressen skal du huske den til internetbaseret login næste gang.

5.2 WAN-indstillinger

Når du har valgt ISP-forbindelse i opsætningsprogrammet og hvis du ønsker at ændre de tilhørende indstillinger, kan du ændre dem og konfigurere indstillingerne her.

Statisk IP

Hvis du har valgt Statisk IP som forbindelse, kan du ændre de følgende adresseinformationer.

- **IP Address**: Indtast en WAN IP-adresse, som du har fået oplyst af din internetudbyder her.
- **Subnet Mask**: Indtast en WAN Subnet-maske her.
- **Gateway**: Indtast en WAN Gateway her.
- **Primary DNS Server**: Indtast den primære DNS-server, som du har fået oplyst af din internetudbyder.
- **Secondary DNS Server**: Indtast den sekundære DNS.

Afsnit 6: Indstilling for trådløs

6.1 Grundlæggende indstillinger

- **Enable Wireless**: Marker for at aktivere routerens trådløse funktioner; fjerne markeringen for at deaktivere dem.
- **Network Mode**: Vælg en funktion blandt de følgende. Standardfunktionen er 11 b/g/n.
- **Main SSID**: SSID (Service Set Identifier) er det unikke navn for det trådløse netværk. Enheden har to SSIDer og det er nødvendigt at have en Main SSID.
- **Minor SSID**: Dette er valgfrit.

- **Broadcast (SSID)**: Vælg ”Enable” for at aktivere enhedens SSID til at være synlig for trådløse klienter. Standardindstillingen er som aktiveret.
- **MBSSID AP Isolation**: En funktion til adgangskontrol baseret på en trådløs MAC-adresse. Hvis denne funktion er aktiveret, kan trådløse klienter forbundet med den samme SSID ikke kommunikere med hinanden.
- **AP Isolation**: En funktion til adgangskontrol baseret på SSID. Hvis denne funktion er aktiveret, vil alle dine trådløse klienter befinde sig i sit eget virtuelle netværk og kan ikke kommunikere med hinanden. Hvis funktionen er aktiveret, kan de trådløse klienter, der er tilsluttet din Main SSID og Minor SSID ikke kommunikere med hinanden, hvilket er en stærk sikkerhed for det trådløse netværk.
- **Channel**: Specificer den effektive kanal (fra 1 til 13/Auto) i det trådløse netværk.
- **Extension Channel**: For at forøge datamængden i det trådløse netværk bruges omfanget af den udvidelseskanal i funktionen 11n.
- **Channel Bandwidth**: Vælg kanalens båndbredde for at forbedre den trådløse ydelse. Hvis netværket har 11 b/g og 11n klienter, kan du vælge 40M; hvis det er et 11n netværk, så vælg 20/40M for at forbedre datamængden.

6.2 Trådløse sikkerhedsindstillinger

Dette bruges til at konfigurere AP-netværkets sikkerhedsindstillinger. Her præsenteres seks (ud af ialt 10) gængse krypteringsmetoder, herunder Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2-enterprise osv.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy) er en grundlæggende krypteringsmetode, der som regel krypterer trådløse data ved hjælp af en række digitale nøgler (64 bits eller 128 bits i længde). Ved at bruge de samme nøgler på hver af enhederne i dit trådløse netværk kan du forhindre uautoriserede trådløse enheder i at overvåge dine transmissioner eller i at bruge dine trådløse ressourcer. Vælg Mixed WEP for at gå ind i det følgende vindue:

- **Select SSID**: Vælg SSID (primære SSID eller sekundære SSID) til at konfigurere sikkerhedsindstillingerne i en rullegardinmenu.
- **Security Mode**: I rullegardinmenuen vælger du de tilsvarende sikkerhedskrypteringsfunktioner.
- **WEP Key1~4**: Indstil WEP-nøglen med ASCII og Hex format. Du kan indtaste en ASCII-kode (5 eller 13 ASCII-tegn. Tegn som f.eks. ”/” er ikke tilladt.) eller 10/26 hex-tegn.
- **Default Key**: Vælg en nøgle blandt de fire konfigurerede nøgler som den aktuelt tilgængelige.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), en Wi-Fi standard, er en nyere trådløs krypteringsfunktion, der er beregnet på at forbedre sikkerhedsfunktionerne i WEP. Det anvender mere effektive krypteringstyper (som f.eks. TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]) og det kan ændre nøglerne dynamisk for hver autoriseret trådløs enhed.

- **Select SSID**: Vælg SSID (primære SSID eller sekundære SSID) til at konfigurere sikkerhedsindstillingerne i en rullegardinmenu.
- **WPA Algorithms**: Giver TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardindstillingen er TKIP.
- **Pass Phrase**: Indtast de krypterede tegn med 8-63 ASCII-tegn.
- **Key Renewal Interval**: Indstil fornyelsesperioden for nøglen.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) giver en højere sikkerhed end WEP (Wireless Equivalent Privacy) og WPA (Wi-Fi Protected Access).

- **Select SSID**: Vælg SSID (primære SSID eller sekundære SSID) til at konfigurere sikkerhedsindstillingerne i en rullegardinmenu.

- **WPA Algorithms**: Giver TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardindstillingen er TKIP.
- **Pass Phrase**: Indtast de krypterede tegn med 8-63 ASCII-tegn.
- **Key renewal Interval**: Indstil fornyelsesperioden for nøglen.

6.2.4 WPA- Enterprise

Denne sikkerhedsfunktion bruges, hvis der er tilsluttet en RADIUS-server til enheden. Vælg ”WPA-Enterprise” i rullegardinmenuen for at gå ind i det følgende vindue:

- **Select SSID**：Vælg SSID (primære SSID eller sekundære SSID) til at konfigurere sikkerhedsindstillingerne i en rullegardinmenu.
- **WPA Algorithms**：Giver TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardindstillingen er TKIP.
- **Key Renewal Interval**: Indstil fornyelsesperioden for nøglen.
- **Radius Server**: Indtast IP-adressen for Radius-serveren.
- **Radius Server port**: Indtast autenticeringsporten for Radius-serveren. Standardindstillingen er 1812.
- **Shared Secret**: Indtast den delte nøgle for autenticeringsserveren med 8-63 ASCII-tegn.
- **Session Timeout**: Autenticerings-intervaltid mellem AP og autenticeringsserveren.

6.2.5 WPA2-Enterprise

Denne sikkerhedsfunktion er baseret på en Radius autenticeringsserver og WPA2 krypteringsmetoden. WPA2 bruges, hvis der er tilsluttet en RADIUS-server til enheden. Vælg ”WPA2-Enterprise” i rullegardinmenuen for at gå ind i det følgende vindue:

- **Select SSID**: Vælg SSID (primære SSID eller sekundære SSID) til at konfigurere sikkerhedsindstillingerne i en rullegardinmenu.
- **WPA Algorithms**: Giver TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardindstillingen er TKIP.
- **Key Renewal Interval**: Indstil fornyelsesperioden for nøglen.
- **Radius Server**: Indtast IP-adressen for Radius-serveren.
- **Radius Server port**: Indtast autenticeringsporten for Radius-serveren. Standardindstillingen er 1812.
- **Shared Secret**: Indtast den delte nøgle for autenticeringsserveren med 8-63 ASCII-tegn.
- **Session Timeout**: Autenticerings-intervaltid mellem AP og autenticeringsserveren. Standardindstillingen er 3600s.

6.2.6 802.1X

Denne sikkerhedsfunktion bruges, hvis der er tilsluttet en RADIUS-server til enheden. 802.1x er en slags port-baseret autenticeringsprotokol og er en autenticeringstype og -strategi for brugerne. Porten kan være enten en fysisk port eller en logisk port (som f.eks. VLAN). For trådløse LAN-brugere er en port blot en kanal. Det endelige formål med 802.11x autenticering er at kontrollere, om porten kan anvendes. Hvis porten autenticeres, kan du åbne denne port, som tillader alle meddelelser at passere. Hvis porten ikke autenticeres, kan du bevare denne port som ”deaktiveret”, hvilket indebærer, at kun 802.1x autenticeringsprotokol-meddelelser kan passere. Vælg ”802.1x” i rullegardinmenuen for at gå ind i det følgende vindue:

- **Select SSID**: Vælg SSID (primære SSID eller sekundære SSID) til at konfigurere sikkerhedsindstillingerne i en rullegardinmenu.
- **WEP**: Klik på ”Enable/Disable” for at aktivere eller deaktivere WEP-algoritmen.
- **Radius Server**: Indtast IP-adressen for Radius-serveren.
- **Radius Server Port**: Indtast autenticeringsporten for Radius-serveren. Standardindstillingen er 1812.
- **Shared Secret**: Indtast den delte nøgle for autenticeringsserveren med 8-63 ASCII-tegn.

- **Session Timeout**: Autenticerings-intervaltid mellem AP og autenticeringsserveren. Standardindstillingen er 3600s.

6.4 WPS-indstillinger

WPS (Wi-Fi Protectec Setting) kan anvendes til på nem og hurtig måde at etablere en forbindelse mellem det trådløse netværks klienter og enheden gennem krypteret indhold. Brugerne skal blot indtaste en PIN-kode eller trykke på WPS-knappen på panelet for at konfigurere det uden manuelt at skulle foretage et valg af krypteringsmetode og hemmelige nøgler. I menuen for "Wireless settings" klikker du på "WPS settings" for at gå ind på næste skærm.

- **WPS settings**: Til at aktivere eller deaktivere WPS-funktionen. Standardindstillingen er "disable" (deaktiveret).
- **WPS mode**: Giver to muligheder: PBC (Push-Button Configuration) og PIN-kode.
- **PBC**: Vælg PBC eller tryk på WPS-knappen på enhedens frontpanel i omkring et sekund. Ttryk på knappen i omkring et sekund, og WPS-indikatoren blinker da i 2 minutter, hvilket betyder at WPS er aktiveret. Men lyset blinker kan du aktivere endnu en enhed for at implementere WPS/PBC kommunikationen mellem dem. Efter to minutter slukker WPS-indikatoren, hvilket betyder at WPS-forbindelsen er fuldført. Hvis der skal tilføjes flere klienter, så gentag ovenstående trin. Aktuelt understøtter WPS adgang for op til 32 klienter.
- PIN: Hvis den valgmulighed aktiveres skal du indtaste en PIN-kode for den trådløse klient i det pågældende felt og bevare den samme kode i WPS-klienten.

6.5 WDS-indstillinger

WDS (Wireless Distribution System) bruges til at udvide det trådløse dækningsområde. Routeren giver tre indstillinger: Lazy, Bridge og Repeater.

Lazy: I denne funktion kan den tilsluttede enhed stå i Bridge-indstilling eller Repeater-indstilling og gå ind i routerens BSSID for at oprette forbindelsen.

Bridge: I denne funktion kan du trådløst tilslutte to eller flere kabelnetværk. I denne funktion skal du tilføje den tilsluttede enheds Wireless MAC-adresse i routerens AP MAC adressetabel eller vælge en fra scanningstabellen.

Repeater Mode: I denne funktion kan du tilføje den tilsvarende MAC-adresse i hver enkelt AP MAC adressetabel manuelt eller via en scanner for at forstørre og udvide det trådløse omfang.

Afsnit 7: DHCP-server

7.1 DHCP-indstillinger

DHCP (Dynamic Host Control Protocol) tildeler en IP-adresse til computere i et LAN/privat netværk. Når du aktiverer DHCP-serveren, vil DHCP-serveren automatisk tildele en ubrugt IP-adresse fra en IP-adressemængde til den anmodende computer, når denne har aktiveret "Obtain an IP Address Automatically" (Få automatisk en IP-adresse). Det er derfor nødvendigt at specificere start- og slutadresse i IP-adressemængden.

- **DHCP Server**: Tjek markeringsfeltet for at aktivere DHCP-serveren.
- **IP Address Start/End**: Indtast IP-adressens omfang for DHCP-server distribution.
- **Lease Time**: Længden på IP-adressens lease.

Afsnit 8: Opgradering af firmware

8.1 Routeren sørger for opgradering af firmware ved et klik på "Upgrade", når du har fundet opgraderingspakken for den pågældende firmware, som kan downloades på www.nedis.nl

- **Browse**: Klik på denne knap for at vælge opgraderingsfilen.
- **Upgrade**: Klik på denne knap for at starte opgraderingsprocessen. Når opgraderingen er fuldført, genstarter routeren automatisk.

8.2 Genstart routeren

Ved at genstarte routeren aktiveres de konfigurerede indstillinger eller routeren indstilles igen, hvis indstillingerne mislykkedes.

8.3 Ændring af password

Denne sektion er til indstilling af nyt brugernavn og password for at give en større sikkerhed for router og netværk.

- **User Name**: Indtast et nyt brugernavn for enheden.
- **Old Password**: Indtast det gamle password.
- **New Password**: Indtast det nye password.
- **Re-enter to Confirm**: Genindtast for at bekræfte det nye password.

8.4 Log af

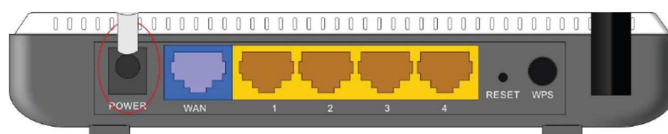
Når du har fuldført alle indstillingerne, så klik på "Yes" på log af siden for at logge af fra indstillingssiden.

Installation og opsætning af router til kabel eller ADSL modem

Forsigtig!

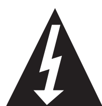
Følg hele vejledningen uden at springe noget trin over

1. Sluk dit modem (tag stikket ud af stikkontakten).
2. Sluk din PC/laptop.
3. Forbind **LAN-udgangen** på dit modem via et **LAN-kabel** til den **blå port** på routeren.
4. Forbind en af de **gule porte** via et **LAN-kabel** til din PC/laptop.



5. Tænd nu dit modem og vent, indtil det har logget på netværket (dette kan tage lidt tid).
6. Tænd routeren og vent i mindst 30 sekunder.
7. Tænd din PC/laptop og vent til den er startet helt op.
8. Åben din browser og gå ind på siden http://192.168.0.1.
9. Indtast dit brugernavn og adgangskode (begge er som standard sat til: **admin**).
10. Åben opsætningsguiden **Setup Wizzard** og klik på **Auto Detect**.
11. Klik nu på **Next** og klik dernæst på **Apply** i næste skærmbillede.
12. Gå ind i menuen **WLAN settings** og kontrollér, at **Enable Wireless** er markeret.
13. Her kan du konfigurere netværkets navn (SSID) og kanal.
14. Gå til undermenuen **Security Settings** og vælg sikkerhedstype. Vi anbefaler, at du altid vælger **Mixed WPA/WPA2 – Personal**.
15. Vælg **WPA Algorithms** og vælg indstillingen **TKIP&AES**.
16. Indsæt din nye adgangskode i feltet **Pass Phrase**. Vi anbefaler, at du vælger en stærk kode bestående af både bogstaver og tal samt helst et eller flere specialtegn.
17. Klik på **Apply** for at gemme dine data.
18. Luk browser-vinduet; opsætning af dit trådløse netværk og sikkerhedsindstillinger er nu gennemført. Hvis du vil, kan du nu fjerne kablet mellem router og PC/laptop og anvende den trådløse forbindelse (såfremt din PC/laptop er udstyret med en trådløs modtager).

Sikkerhedsforholdsregler:






For at nedsætte risikoen for elektrisk stød, må dette produkt, f.eks. når der kræves service, KUN åbnes af en autoriseret tekniker. Frakobl produktet stikkontakten og andet udstyr, hvis der opstår et problem. Udsæt ikke produktet for vand eller fugt.

Vedligeholdelse:

Rengør kun med en tør klud. Brug ikke opløsningsmidler eller slibende rengøringsmidler.

Garanti:

Ingen garanti og ikke noget ansvar kan påtages for ændringer af produktet eller for skade på grund af forkert brug af dette produkt.

Generelt:

- Design og specifikationer kan ændres uden varsel.
- Alle bomærker og produktnavne er varemærker eller registrerede varemærker tilhørende deres respektive ejere og anses herved som sådan.
- Denne vejledning blev udført omhyggeligt. Imidlertid kan der ikke afledes nogen rettigheder. König Electronic kan ikke holdes ansvarlig for eventuelle fejl i denne vejledning eller deres konsekvenser.
- Gem brugervejledningen og emballagen til senere brug.

Bemærk:



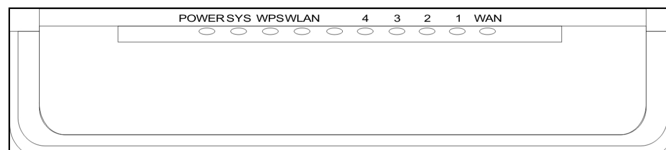
Dette produkt er mærket med dette symbol. Det betyder, at brugt elektrisk og elektronisk udstyr ikke må bortskaffes sammen med almindeligt husholdningsaffald. Der findes særlige indsamlingssystemer for disse produkter.

NORSK

Kapittel 1: Introduksjon

1.1 LED-indikatorer og portbeskrivelse

Frontpanel og LED-indikatorer



Beskrivelse av LED-indikatorer på frontpanelet: (fra V til H)

- **POWER (STRØM)**

  Når det grønne lyset er på, indikerer det at strømmen er riktig tilkoblet.
- **SYS**

  Når det grønne lyset blinker, indikerer det at systemet kjører som det skal.
- **WPS**

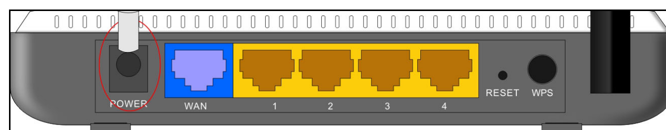
  Når det blinker, indikerer det at enheten forhandler med klienten i WPS-modus.
- **WLAN**

  LED-indikator for trådløst signal. Når det grønne lyset blinker, indikerer det at den trådløse funksjonen er aktivert.
- **LAN (4, 3, 2, 1)**

  LED-indikator for lokalt kabelnettverk. Dersom det lyser, indikerer det at det er tilkoblet Ethernet-enheten; blinker det, indikerer det at enheten overfører og/eller mottar data.
- **WAN**

  LED-indikator for fjernnett. Dersom det lyser, indikerer det routerens W.

Beskrivelse av endepanel:



Endepanel: (Fra V til H)

- **POWER (STRØM)**

Inngangen er for tilkobling av strømadapteren. Vennligst bruk 9V likestrøms-adapteren som medfølger.

- **WAN**

En 100Mbps Ethernet-port som kan tilkobles modem, switch, router og andre Ethernet-enheter for tilkobling til DSL-modem, kabel-modem og ISP.

- **LAN (1, 2, 3, 4)**

Fire 10/100Mbps Ethernet-porter som kan tilkobles Ethernet-switch, Ethernet-router og NIC-kort.

- **RESET**

Systemnullstillingsknappen. Ved å holde denne knappen inne i syv sekunder vil de konfigurerte innstillingene i enheten slettes og standardinnstillingene vil gjenopprettes.

- **WPS**

Hold den inne i ett sekund og WPS-funksjonen vil aktiveres og WPS-indikatoren vil blinke.

Kapittel 2: Installasjon av maskinvare

2.1 Hvordan installere routeren

Vennligst bruk adapteren som medfølger for å forsyne strøm til routeren. VIKTIG: Bruk av en annen strømadapter kan skade enheten og ugyldiggjøre garantien for dette produktet. Vennligst bruk en kabel for å koble LAN-porten til routeren til nettverksadapteren til datamaskinen din. Vennligst koble bredbåndslinjen din, levert av ISP-en din, til WAN-porten. Sett inn CD-en som medfølger i CD-ROM-driveren, dobbeltklikk på «Setup»-ikonet og følg instruksjonene for å fullføre installasjonen. Eller så kan du gå inn på routerens nettside for å konfigurere den. (For flere detaljer, vennligst se kapittel 3.)

Kapittel 3: Hvordan logge inn på routeren

3.1 Hvordan stille inn nettverkskonfigurasjoner

1. På skrivebordet til datamaskinen din, høyre-klikk ”Mine nettverkssteder” og velg ”Egenskaper”.
2. Høyre-klikk ”LAN-tilkobling” og velg ”Egenskaper”.
3. Velg ”Internett-protokoll (TCP/IP)” og klikk på ”Egenskaper”.
4. - Velg ”Skaff en IP-adresse automatisk” og ”Skaff en DNS-serveradresse automatisk”. Klikk ”OK” for å lagre konfigurasjonene.
   - Eller velg ”Bruk følgende IP-adresse” og skriv inn IP-adressen, Subnet-masken og standard Gateway som følger: IP-adresse: 192.168.0.XXX: (XXX er et nummer fra 2~254) Subnet-maske: 255.255.255.0. Gateway: 192.168.0.1. Du er nødt til å skrive inn DNS-serveradressen du fikk av ISP-en din. Ellers kan du bruke routerens standard Gateway som DNS-proxyserveren. Klikk ”OK” for å lagre konfigurasjonene.

3.2 Logge inn på routeren

1. For å få tilgang til routerens nettbaserte grensesnitt, skriv inn routerens standard IP-adresse (http://192.168.0.1) i en nettleser, som f.eks. Internet Explorer eller Google Chrome.
2. Skriv ”admin” i feltene for både brukernavn og passord. Klikk ”OK”.

Standard innstillinger	
IP-addresse	192.168.0.1
Passord	admin
SSID	KONIG
Sikkerhetsmodus	Deaktivert
Trådløs modus	b/g/n Mixd-modus
Kanal	Auto-valg
Tidssone	
WPS-innstillinger	Aktivert
UPNP-enhetsnavn	11N Wireless Broadband Router
UPNP-produsent	KONIGELECTRONIC
UPNP-modellnavn	CMP-WNROUT41
UPNP-modellnummer	V 1.0
UPNP-rapportert nettverkshastighet	300Mbps
UPNP-enhetsadresse	http://192.168.0.1
UPNP	Deaktivert

Kapittel 4: Hurtiginstallasjonsveiviser

4.1 Installasjonsveiviser

Her er ”Velkommen til installasjonsveiviseren” for rask konfigurasjon av routeren din. Klikk ”Neste”.

I dette skjermbildet, velg internett-tilkoblingsmodusen din bruker. Dersom du ikke er sikker, trykk på ”Søk”-knappen eller kontakt din internettleverandør, og klikk ”Neste”.

ADSL, virtuell oppringning (Via PPPoE)

Skriv inn kontoen og passordet levert av ISP-en din, og klikk ”Neste”.

Dynamisk IP (Via DHCP)

Dersom tilkoblingsmodusen din er dynamisk IP, vil det si at IP-adressen din endrer seg hver gang du kobler deg på. Du trenger ikke skrive inn informasjon som du må med andre moduser. Klikk ”Neste” og ”Lagre” for å fullføre innstillingene.

Statisk IP

I dette skjermbildet, skriv inn nettverksadresseinformasjon fra ISP-en din i feltene for IP-adresse, Subnet-maske, Gateway og primær-DNS-server, og klikk ”Neste”.

L2TP

Ta kontakt med ISP-en din for den nødvendige informasjonen.

Kapittel 5: Avanserte innstillinger

5.1 LAN-innstillinger

LAN-innstillinger er for de grunnleggende TCP/IP-parameterne til LAN-portene.

- **IP-adresse**: Routerens LAN-IP-adresse (ikke IP-adressen til datamaskinen din). 192.168.0.1 er standardverdien.
- **Subnet-maske**: Den viser routerens Subnet-maske for måling av nettverksstørrelsen. 255.255.255.0 er standardverdien.

VIKTIG:

Når du endrer IP-adressen er du nødt til å huske den for det nettbaserte verktøyet neste gang.

5.2 WAN-innstillinger

Etter at du har valg ISP-forbindelsestypen i ”Installasjonsveiviseren” og du ønsker å endre de relaterte innstillingene, kan du endre og konfigurere innstillingene i detalj her.

Statisk IP

Dersom du har valg statisk IP som tilkoblingsmodus, kan du endre følgende adresse-informasjon.

- **IP-adresse**: Skriv inn WAN-IP-adressen levert av ISP-en din her.
- **Subnet-maske**: Skriv inn WAN-Subnet-masken her.
- **Gateway**: Skriv inn WAN-Gateway her.
- **Primær DNS-server**: Skriv inn primær-DNS-serveren levert av ISP-en din.
- **Sekundær DNS-server**: Skriv inn sekundær-DNS.

Kapittel 6: Trådløse innstillinger

6.1 Grunnleggende innstillinger

- **Aktiver trådløs funksjon**: Merk for å aktivere routerens trådløse funksjon; avmerk for å deaktivere den.
- **Nettverksmodus**: Velg en modus fra listen. Standarden er 11b/g/n-modus.
- **Hoved-SSID**: SSID (Service Set Identifier) er det trådløse nettverkets unike navn. Denne enheten har to SSID-er og hoved-SSID-en er nødvendig.
- **Annen-SSID**: Denne er valgfri.
- **Kringkasting (SSID)**: Velg ”Aktiver” for å tillate at enhetens SSID er synlig for trådløse klienter. Standardinnstillingen er at den er aktivert.
- **MBSSID AP-isolasjon**: En tilgangskontrollfunksjon basert på trådløs MAC-adresse. Når denne funksjonen er aktivert, kan ikke trådløse klienter tilkoblet samme SSID kommunisere med hverandre.
- **AP-isolasjon**: En tilgangskontrollfunksjon basert på SSID. Når denne funksjonen er aktivert, vil hver av dine trådløse klienter være i sitt eget virtuelle nettverk og vil ikke kunne kommunisere med hverandre.

Trådløse klienter tilkoblet hoved-SSID og annen-SSID kan heller ikke kommunisere med hverandre, noe som kan sikre det trådløse nettverket på sterkt vis.

- **Kanal**: Spesifiser den effektive kanalen (fra 1 til 13\Auto) til det trådløse nettverket.
- **Utvidelseskanal**: For å øke datagjennomstrømmingen til det trådløse nettverket brukes utvidelseskanalen i 11n-modus.
- **Kanalbåndbredde**: Velg kanalbåndbredden for å forbedre den trådløse ytelsen. Når nettverket har 11b/g- og 11n-klienter kan du velge 40M; når det er et 11n-nettverk, velg 20/40M for å forbedre gjennomstrømmingen.

6.2 Sikkerhetsinnstillinger for trådløst nettverk

Dette brukes til å konfigurere AP-nettverkets sikkerhetsinnstillinger. Her er seks (totalt ti) vanlige krypteringsmetoder presentert, inkludert Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, osv.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), en grunnleggende krypteringsmetode, krypterer som regel trådløst data ved bruk av en rekke digitale nøkler (64 bits eller 128 bits i lengde). Ved å bruke den sammen nøkkelen på begge dine trådløse nettverksenheter, kan du hindre uautoriserte trådløse nettverksenheter fra å overvåke dine overførsler eller bruke dine trådløse kilder. Velg Mixed WEP for å komme til følgende vindu:

- **Velg SSID**: Velg SSID-en (hoved-SSID eller annen-SSID) for å konfigurere sikkerhetsinnstillinger fra nedtrekksmenyen.
- **Sikkerhetsmodus**: Fra nedtrekksmenyen, velg de tilsvarende sikkerhetskrypteringsmodusene.
- **WEP-nøkkel 1~4**: Angi WEP-nøkkelen med ASCII- og Hex-format. Du kan skrive inn ASCII-koden (5 eller 13 ASCII-tegn, ugyldige tegn, som "/" er ikke tillatt) eller 10/26 hex-tegn.
- **Standardnøkkel**: Velg en nøkkel fra de fire konfigurerte nøklene som den gjeldende tilgjengelige.

6.2.2 WPA-Personal

WPA (Wi-Fi Protected Access), en Wi-Fi-standard, er en mer nylig trådløs krypteringsordning, utformet for å forbedre sikkerhetsfunksjonene til WEP. Den påfører mer kraftige krypteringstyper (som TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]) og kan endre nøklene dynamisk på hver eneste autoriserte trådløse enhet.

- **Velg SSID**: Velg SSID-en (hoved-SSID eller annen-SSID) for å konfigurere sikkerhetsinnstillinger fra nedtrekksmenyen.
- **WPA-algoritmer**: Leverer TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardmodusen er TKIP.
- **Passordfrase**: Skriv inn de krypterte tegnene med 8-63 ASCII-tegn.
- **Nøkkelfornyelsesintervall**: Angi nøkkelens fornyelsesperiode.

6.2.3 WPA2- Personal

WPA2 (Wi-Fi Protected Access version 2) tilbyr høyere sikkerhet enn WEP (Wireless Equivalent Privacy) og WPA (Wi-Fi Protected Access).

- **Velg SSID**: Velg SSID-en (hoved-SSID eller annen-SSID) for å konfigurere sikkerhetsinnstillinger fra nedtrekksmenyen.
- **WPA-algoritmer**: Leverer TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardmodusen er TKIP.
- **Passordfrase**: Skriv inn de krypterte tegnene med 8-63 ASCII-tegn.
- **Nøkkelfornyelsesintervall**: Angi nøkkelens fornyelsesperiode.

6.2.4 WPA- Enterprise

Denne sikkerhetsmodusen brukes når en RADIUS-server er tilkoblet enheten. Velg ”WPA-Enterprise” fra nedtrekksmenyen for å komme til følgende vindu:

- **Velg SSID**: Velg SSID-en (hoved-SSID eller annen-SSID) for å konfigurere sikkerhetsinnstillinger fra nedtrekksmenyen.
- **WPA-algoritmer**: Leverer TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardmodusen er TKIP.
- **Nøkkelfornyelsesintervall**: Angi nøkkelens fornyelsesperiode.
- **Radius-server**: Angi IP-adressen til Radius-serveren.
- **Radius-serverport**: Anfi autentiseringsporten til Radius-serveren. Standardporten er 1812.
- **Delt nøkkel**: Angi den delte nøkkelen for autentiseringsserveren med 8~63 ASCII-tegn.
- **Tidsavbrudd for økt**: Autentiseringsintervallperioden mellom AP og autentiseringsserveren.

6.2.5 WPA2-Enterprise

Denne sikkerhetsmodusen er basert på Radius-autentiseringsserver og WPA2-krypteringsmetode. WPA2 brukes når en RADIUS-server er tilkoblet enheten. Velg ”WPA2-Enterprise” fra nedtrekksmenyen for å komme til følgende vindu:

- **Velg SSID**: Velg SSID-en (hoved-SSID eller annen-SSID) for å konfigurere sikkerhetsinnstillinger fra nedtrekksmenyen.
- **WPA-algoritmer**: Leverer TKIP [Temporal Key Integrity Protocol] eller AES [Advanced Encryption Standard]. Standardmodusen er TKIP.
- **Nøkkelfornyelsesintervall**: Angi nøkkelens fornyelsesperiode.
- **Radius-server**: Angi IP-adressen til Radius-serveren.
- **Radius-serverport**: Anfi autentiseringsporten til Radius-serveren. Standardporten er 1812.
- **Delt nøkkel**: Angi den delte nøkkelen for autentiseringsserveren med 8~63 ASCII-tegn.
- **Tidsavbrudd for økt**: Autentiseringsintervallperioden mellom AP og autentiseringsserveren. Standardperioden er 3600s.

6.2.6 802.1X

Denne sikkerhetsmodusen brukes når en RADIUS-server er tilkoblet enheten. 802.1x, en type port-basert autentiseringsprotokoll, er en autentiseringstype og –strategi for brukere. Porten kan enten være en fysisk port eller en logisk port (som f.eks. VLAN). For trådløse LAN-brukere er en port kun en kanal. Det endelige formålet med 802.1x-autentisering er å kontrollere om porten kan brukes. Dersom porten blir vellykket autentisert kan du åpne den, noe som tillater alle meldinger å passere. Dersom porten ikke blir vellykket autentisert kan du holde denne porten ”deaktivert”, noe som tillater kun 802.1x-autentiseringsprotokollmeldinger å passere. Velg ”802.1x” fra nedtrekksmenyen for å komme til følgende vindu:

- **Velg SSID**: Velg SSID-en (hoved-SSID eller annen-SSID) for å konfigurere sikkerhetsinnstillinger fra nedtrekksmenyen.
- **WEP**: Klikk ”Aktiver/Deaktiver” for å aktivere eller deaktivere WEP-algoritmen.
- **Radius-server**: Angi IP-adressen til Radius-serveren.
- **Radius-serverport**: Anfi autentiseringsporten til Radius-serveren. Standardporten er 1812.
- **Delt nøkkel**: Angi den delte nøkkelen for autentiseringsserveren med 8~63 ASCII-tegn
- **Tidsavbrudd for økt**: Autentiseringsintervallperioden mellom AP og autentiseringsserveren. Standardperioden er 3600s.

6.4 WPS-innstillinger

WPS (Wi-Fi Protected Setting) kan brukes til enkelt og raskt etablere forbindelsen mellom de trådløse nettverksklientene og enheten gjennom bruk av kryptert innhold. Brukere skriver kun inn en PIN-kode eller

trykker WPS-knappen på panelet for å konfigurere den uten å velge en krypteringsmetode og hemmelige nøkler manuelt. I menyen ”Trådløse innstillinger”, klikk ”WPS-innstillinger” for å komme til neste skjermbilde.

- **WPS-innstillinger**: For å aktivere eller deaktivere WPS-funksjonen. Standarden er ”deaktivert”.
- **WPS-modus**: Tilbyr to måter: PBC (Push-Button Configuration) og PIN-kode.
- **PBC**: Velg PBC eller trykk på WPS-knappen på frontpanelet av enheten og hold inne i omtrent ett sekund. Da vil WPS-indikatoren blinke i to minutter, noe som vil si at WPS-en er aktivert. Mens den blinker kan du aktivere en annen enhet til å implementere WPS-/PBC-forhandlingen mellom dem. Etter to minutter vil WEP-indikatoren slås av, noe som betyr at WPS-tilkoblingen er fullført. Dersom det legges til flere klienter, gjenta de forannevnte stegene. Per dags dato støtter WPS opp til 32 klienter.
- PIN: Dersom dette alternativet er aktivert, er du nødt til å skrive inn en trådløs klients PIN-kode i feltet og bruker den samme koden i WPS-klienten.

6.5 WDS-innstillinger

WDS (Wireless Distribution System) brukes for å utvide det trådløse dekkområdet. Denne routeren tilbyr tre moduser: Lazy, Bridge og Repeater.

Lazy: I denne modusen kan den tilkoblede enheten være i Bridge-modus eller Repeater-modus, og entre routerens BSSID for å etablere forbindelsen.

Bridge: Du kan trådløst tilkoble to eller flere kabelnettverk via denne modusen. I denne modusen er du nødt til å legge til den trådløse MAC-adressen til den tilkoblede enheten i routerens AP MAC-adressetabell eller velge en fra scanner-tabellen.

Repeater: I denne modusen, legg til den motstridende MAC-adressen i hver sin AP MAC-adressetabell manuelt eller via scanner for å forstørre og forlenge den trådløse radiusen.

Kapittel 7: DHCP-server

7.1 DHCP-innstillinger

DHCP (Dynamic Host Control Protocol) tilordner en IP-adresse til datamaskinen på LAN/private nettverk. Når du aktiverer DHCP-serveren vil den automatisk tildele en ubrukt IP-adresse fra IP-adressebassenget til den anmodende datamaskinen på forutsetningen at den aktiverer ”Skaff en IP-adresse automatisk”. Så det er nødvendig å spesifisere start- og endreadressene til IP-adressebassenget.

- **DHCP-server**: Aktiver sjekkboksen for å aktivere DHCP-serveren.
- **IP-adresse, start/ende**: Angi rekkevidden til IP-adresse for DHCP-serverdistribusjon.
- **Leietid**: Lengden til IP-adresseleien.

Kapittel 8: Oppgradere fastvare

8.1 Routeren tilbyr fastvareoppgraderings ved å klikke ”Oppgrader” etter ha bladd gjennom fastvareoppgraderingspakken som du kan laste ned fra www.nedis.nl

- **Bla gjennom**: klikk denne knappen for å velge oppgraderingsfilen.
- **Oppgrader**: klikk denne knappen for å begynne oppgraderingsprosessen. Etter at oppgraderingen er fullført vil routeren automatisk kjøre en omstart.

8.2 Omstarte routeren

Omstart av routeren gjør at de konfigurerte innstillingene trår i kraft eller angir routeren igjen dersom innstillingene mislyktes.

8.3 Passordendring

Denne seksjonen er for innstilling av et nytt brukernavn og passord for å bedre sikre routeren og nettverket ditt.

- **Brukernavn**: Skriv inn et nytt brukernavn for enheten din.
- **Gammelt passord**: Skriv inn det gamle passordet.
- **Nytt passord**: Skriv inn et nytt passord.

- **Gjenta for å bekrefte**: Gjenta passordet for å bekrefte.

8.4 Logg ut

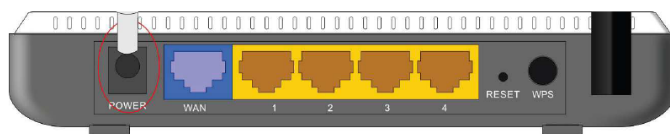
Etter at du har fullført innstillingene, klikk "Ja" på utloggingssiden for å logge ut av nettbehandlingssiden.

Hvordan installere og sette opp en router på et kabel- eller ADSL-modem

Advarsel!

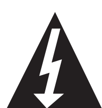
Følg alle disse stegene uten å hoppe over noen

1. Skru av modemet (koble det fra strømkilden).
2. Skru av PC-en.
3. Koble **LAN-utgangen** til modemet via en **LAN-kabel** til den **blå porten** på routeren.
4. Koble en av de **gule portene** via en **LAN-kabel** til PC-en.



5. Skru nå på modemet og vent inntil det er fullstendig påslått (dette kan ta en stund).
6. Skru på routeren og vent i minst 30 sekunder.
7. Skru på PC-en og vent til den er fullstendig påslått.
8. Åpne nettleseren din og naviger deg til http://192.168.0.1.
9. Tast inn brukernavn og passord (standard på begge: **admin**).
10. Naviger deg til **Installasjonsveiviseren** og klikk på **Auto-deteksjon**.
11. Klikk nå på **Neste** og i det følgende skjermbildet, klikk på **Angi**.
12. Naviger deg til menyen **WLAN-innstillinger** og sørg for at **Aktiver trådløst** er huket av.
13. Her kan du konfigurere nettverksnavnet ditt (SSID) og kanalen.
14. Naviger deg til undermenyen **Sikkerhetsinnstillinger** og velg din ønskede sikkerhetstype. Vi anbefaler alltid å velge **Blandet WPA/WPA2 – Personlig**.
15. Sett **WPA-algoritmene** til å være **TKIP&AES**.
16. Endre passordet i feltet **Passordfrase**. Vi anbefaler at du oppretter et sterkt passord som består av bokstaver, tall og kanskje også et spesialtegn.
17. Klikk på **Angi** for å lagre dataene.
18. Avslutt nettleseren din; dine trådløse nettverks- og sikkerhetsinnstillinger er fullførte. Alternativt kan du koble fra kabelen mellom routeren og PC-en for å koble til en trådløs forbindelse (dersom PC-en er utstyrt med en trådløs mottaker).

Sikkerhetsforholdsregler:







For å redusere faren for strømstøt, skal dette produktet BARE åpnes av en autorisert tekniker når vedlikehold er nødvendig. Koble produktet fra strømmen og annet utstyr dersom et problem oppstår. Ikke utsett produktet for vann eller fuktighet.

Vedlikehold:

Rens bare med en tørr klut. Ikke bruk rensemidler eller skuremidler.

Garanti:

Ingen garanti eller erstatningsansvar aksepteres ved endringer og modifiseringer av produktet eller skade forårsaket av uriktig bruk av dette produktet.

Generelt:

- Utforming og spesifikasjoner kan endres uten forhåndsvarsel.
- Alle logoer, merker og produktnavn er varemerker eller registrerte varemerker til de respektive eierne, og skal behandles som dette.
- Denne manualen ble laget med omhu. Imidlertid kan ingen rettigheter utledes. König Electronic kan ikke ta ansvar for eventuelle feil i denne manualen eller konsekvenser som følger.
- Behold denne veiledningen og innpakningen for fremtidig referanse.

Forsiktig:



Dette produktet er markert med dette symbolet. Det betyr at brukte elektriske og elektroniske produkter ikke må blandes med vanlig husholdningsavfall. Det finnes egne innsamlingssystem for slike produkter.



Declaration of conformity / Konformitätserklärung / Déclaration de conformité / Conformiteitsverklaring / Dichiarazione di conformità / Declaración de conformidad / Megfelelőségi nyilatkozat / Yhdenmukaisuusvakuutus / Överensstämmelseförklaring / Prohlášení o shodě / Declarație de conformitate / Δήλωση συμφωνίας / Overensstemmelse erklæring / Overensstemmelse forklaring

We, / Wir, / Nous, / Wij, / Questa società, / La empresa infrascrita, / Mi, / Me, / Vi, / Společnost, / Noi, / Εμείς
Nedis B.V., De Tweeling 28, 5215MC, 's-Hertogenbosch
The Netherlands / Niederlande / Pays Bas / Nederland / Paesi Bassi / Países Bajos / Hollandia / Alankomaat / Holland / Nizozemí / Olanda / Ολλανδία
Tel. / Tél / Puh / Τηλ. : 0031 73 5991055
Email / Couriel / Sähköposti / e-post: info@nedis.com

Declare that product: / erklären, dass das Produkt: / Déclarons que le produit : / verklaren dat het product: / Dichiara che il prodotto: / Declara que el producto: / Kijelentjük, hogy a termék, amelynek: / Vakuutamme, että: / Intygar att produkten: / prohlašuje, že výrobek: / Declarăm că acest produs: / Δηλώνουμε ότι το προϊόν: / Erklærer at produktet: / Forsikrer at produktet:

Brand: / Marke: / Marque : / Merknaam: / Marca: / Márkája: / Merkki: / Märke: / Značka: / Μάρκα: / Mærke: / Merke: **KÖNIG ELECTRONIC**
Model: / Modell: / Modèle : / Modello: / Modelo: / Típusa: / Malli: / Μοντέλο: **CMP-WNROUT41**

Description:	Wireless 11N router 300M
Beschreibung:	11n WLAN Router 300 MBit
Description :	Routeur de réseau sans fil 11N 300M
Omschrijving:	Draadloze 11N router 300M
Descrizione:	Router Wireless 11N 300M
Descripción:	Router inalámbrico 11N 300M
Megnevezése:	Vezeték nélküli 11N útválasztó 300M
Kuvaus:	Langaton 11N reititin 300M
Beskrivning:	Trådlös router 11N 300 m
Popis:	Bezdrátový 11N router 300M
Descriere:	Router wireless 11N 300M
Περιγραφή:	Ασύρματο router 11N 300M
Beskrivelse:	Wireless 11N router 300M
Beskrivelse:	Trådløs 11N router 300M

Is in conformity with the following standards: / den folgenden Standards entspricht: / est conforme aux normes suivantes : / in overeenstemming met de volgende normen is: / è conforme ai seguenti standard: / es conforme a las siguientes normas: / Megfelel az alábbi szabványoknak: / Täyttää seuraavat standardit: / Överensstämmer med följande standarder: / splňuje následující normy: / Este în conformitate cu următoarele standarde: / Συμμορφώνεται με τις ακόλουθες προδιαγραφές: / Overensstemmelse med følgende standarder: / Overensstemmer med følgende standarder:
EN60950-1:2006+A11:2009+A1:2010
EN55022:2006+A1:2007
EN61000-3-2:2006+A1:2009+A2:2009
EN61000-3-3:2008
EN61000-4-2:2009
EN61000-4-3:2006+A1:2008+A2:2010
EN61000-4-4:2004+A1:2010
EN61000-4-5:2006
EN61000-4-6:2009
EN61000-4-11:2004
EN50371:2002

EU Directive(s) / EG-Richtlinie(n) / Directive(s) EU / EU richtlijn(en) / Direttiva(e) EU / Directiva(s) UE / EU direktívák / EU Toimintaohje(et) / Eu Direktiv(en) / Směrnice EU / Directiva(e) UE / Οδηγία(ες) της ΕΕ / EU direktiv(er) / EU-direktiv(ene): **1999/5/EC, 2006/95/EC, 2004/108/EC, 2002/95/EC**

‘s-Hertogenbosch, **24-12-2011**
Mr. / Hr. / M. / Dhr. / Sig. / Sr. D. / Úr / Mr. / Herr. / Pan / Dl. / K. / Hr. / Herr:
Randolf Richardson
Chief Operating Officer / Geschäftsführer / Chef des operations / Operationeel Directeur / Responsabile Operativo / Director de Operaciones / Üzemviteli Igazgató / Käyttöpäällikkö / Driftschef / Provozní ředitel / Director principal / Γενικός Διευθυντής Επιχειρήσεων / Chief Operating Officer / Administrerende Driftsdirektør

NEDIS B.V.
Postbus 70509, 5201 CZ 's-Hertogenbosch NL
De Tweeling 28, 5215 MC 's-Hertogenbosch NL
Telefoon: 073 - 599 10 55